Sun Java™ System Identity Manager Versionshinweise

Version 7.0 November 2006

Teile.-Nr. 820-0158-10

Diese Versionshinweise enthalten wichtige Informationen, die zum Zeitpunkt der Veröffentlichung von Sun Java System Identity Manager 7.0 verfügbar waren. In diesem Dokument werden neue Leistungsmerkmale und Erweiterungen, bekannte Probleme und Einschränkungen sowie weitere Informationen behandelt. Vor der Arbeit mit Identity Manager 7.0 sollten Sie dieses Dokument lesen.

In diesem Dokument sind URLs von Drittparteien aufgeführt, unter denen Sie zusätzliche zugehörige Informationen finden.

HINWEIS Sun ist nicht verantwortlich für die Verfügbarkeit der in diesem Dokument erwähnten Websites anderer Hersteller. Inhalt, Werbungen, Produkte oder anderes Material, das auf oder über diese Sites oder Ressourcen verfügbar ist, drücken weder die Meinung von Sun aus, noch ist Sun für diese verantwortlich. Sun lehnt jede Verantwortung oder Haftung für direkte oder indirekte Schäden oder Verluste ab, die durch die bzw. in Verbindung mit der Verwendung von oder der Stützung auf derartige Inhalte, Waren oder Dienstleistungen, die auf oder über diese Sites oder Ressourcen verfügbar sind, entstehen können.

Unterstützte Software und Umgebungen

In diesem Abschnitt werden die Softwareprodukte und Umgebungen aufgelistet, die mit der Identity-Produktsoftware kompatibel sind:

- Betriebssysteme
- Anwendungsserver
- Browser
- Repository-Datenbankserver
- Sun Identity Manager Gateway
- Unterstützte Ressourcen
- Webserver
- Nicht mehr unterstützte Software

HINWEIS Da die Entwickler der Softwareprodukte häufig neue Versionen, Aktualisierungen und Korrekturen herausbringen, sind die hier veröffentlichten Informationen häufig Änderungen unterworfen. Lesen Sie deshalb vor der Installation die jeweiligen Versionshinweise.

Betriebssysteme

Diese Version von Identity Manager unterstützt die folgenden Betriebssysteme:

- AIX 4.3.3, 5.2, 5L v5.3
- HP-UX 11i v1, 11i v2
- Microsoft Windows 2000 SP3 oder höher
- Microsoft Windows 2003
- Solaris 8, 9, 10 SPARC und x86d
- Red Hat Linux Advanced Server 2.1
- Red Hat Linux Enterprise Server 3.0, 4.0
- Novell SuSE Linux Enterprise Server 9 SP1

Anwendungsserver

Der Anwendungsserver, den Sie mit Identity Manager verwenden, muss Servlet 2.2 unterstützen und mit der enthaltenen Java-Plattform installiert werden (sofern nicht anders angegeben). Identity Manager erfordert JDK 1.4.2 oder höher.

- Apache® Tomcat
  - Version 4,1.x (mit JDK 1.4.2)
  - Version 5.0.x (mit JDK 1.4.2)
  - Version 5.5.x (mit JDK 1.5)
- BEA WebLogic® Express 8.1 (mit JDK 1.4.2 oder höher)
- BEA WebLogic® Express™ 8.1 (mit JDK 1.4.2 oder höher)
- BEA WebLogic® Server™ 9
- IBM WebSphere® 6.0
- IBM WebSphere® Application Server - Express Version 5.1.1 (mit JDK 1.4.2)
- JBoss Application Server 4.0.4
- Sun™ ONE Application Server 7
- Sun Java™ System Application Server Platform Edition 8
- Sun Java™ System Application Server Platform Edition und Enterprise Edition 8.1

HINWEIS Wenn Ihr derzeitiger Anwendungsserver JDK 1.4.2 oder höher nicht unterstützt, sollten Sie sich beim Hersteller vor der Installation von Identity Manager 7.0 über die Auswirkungen der Aufrüstung auf eine Version, die JDK 1.4.2 oder höher unterstützt, erkundigen.

Browser

Identity Manager unterstützt die folgenden Browser:

- Microsoft Internet Explorer 5.x oder höher
- Safari v2.0 oder höher für Mac OS X 10.3.3 oder höher
- Mozilla 1.78 (mit JRE 1.5)
- Firefox 1.04, 1.05, 1.06, 1.5 (mit JRE 1.5)

Repository-Datenbankserver

Identity Manager unterstützt die folgenden Repository-Datenbankserver:

- IBM® DB2® Universal Database für Linux, UNIX® und Windows® (Version 7.x, 8.1, 8.2)
- Microsoft SQL Server™ 2000, 2005
- MySQL™ 4.1, 5.0
- Oracle 9i® und Oracle Database 10g, 10g Release 1 und 10g Release 2®

Sun Identity Manager Gateway

Wenn Sie Windows Active Directory, Novell NetWare, Novell GroupWise, Exchange 5.5, Remedy, Lotus Domino oder RSA ACE/Server einrichten möchten, müssen Sie Sie vorher Sun Identity Manager Gateway installieren.

Unterstützte Ressourcen

Identity Manager unterstützt die folgenden Ressourcen:

- CRM (Customer Relationship Management)
- Datenbanken
- Enterprise Resource Planning (ERP)
- Help Desk
- Messaging-Plattformen
- Message-Queue
- Betriebssysteme
- Rollenmanagement
- Sicherheitsmanager
- Steuerung des Webzugriffs

CRM (Customer Relationship Management)

- Siebel CRM-Software Version 6.2, 7.0.4, 7.7, 7.8

Datenbanken

- Generische Datenbanktabellen
- IBM® DB2® Universal Database für Linux, UNIX® und Windows® (7.x, 8.1, 8.2)
- Microsoft® Identity Integration Server (MIIS) 2003
- Microsoft SQL Server 2000, 2005
- MySQL™ 4.1.*x*, 5.*x*
- Oracle 9i®
- Oracle Database 10g Release 1®
- Sybase Adaptive Server® 12.*x*
- Skript-JDBC

Verzeichnisse

- LDAP v3
- Microsoft® Active Directory® 2000, 2003
- Novell® eDirectory für Novell NetWare 5.1, 6.0
- Open LDAP
- Sun™ ONE Directory Server 4.*x*
- Versionshinweise für Sun Java™ SystemDirectory Server 5 2004Q2, 2005Q1

HINWEIS

- Identity Manager wird auf Sun™ ONE Directory Server und Open LDAP getestet. LDAP-Server, die v3 unterstützen, können deshalb ohne Änderungen des Ressourcenadapters ausgeführt werden.
- Für Sun Java™ System Directory Server 5 2005Q1 muss ein Patch für das Plugin „retro changelog“ von Directory Server installiert werden, wenn Sie ActiveSync verwenden. Das Patch ist nur für die „regelmäßige“ Replikation erforderlich (nicht für die MMR-Replikation).

Enterprise Resource Planning (ERP)

- Oracle E-Business Suite on Oracle Applications 11.5.9, 11.5.10
- Peoplesoft® PeopleTools 8.1 bis 8.4.2 mit HRMS 8.0 bis 8.8
- SAP® R/3 v4.5, v4.6
- SAP® R/3 Enterprise 4.7 (SAP BASIS 6.20)
- SAP® NetWeaver Enterprise Portal 2004 (SAP BASIS 6.40)
- SAP® NetWeaver Enterprise Portal 2004s (SAP BASIS 7.00)

Help Desk

- Remedy® Help Desk 4.5, 5.0.

Messaging-Plattformen

- Blackberry RIM Enterprise Server 4+ (verwendet Generic Windows Script Adapter)
- Sun Java System Messaging and Calender Service
- Lotus Notes® 5.0, 6.5, 6.5.4 (Domino)
- Microsoft® Exchange 5.5, 2000, 2003
- Novell® GroupWise 5.*x*, 6.0

HINWEIS

- Microsoft Exchange 2000 und 2003 werden von Microsoft Windows Active Directory 2000 und 2003 verwaltet.
- Der BlackBerry-Ressourcenadapter wird in künftigen Versionen nicht mehr unterstützt. Zukünftige Implementierungen, die Ressourcenadapter für Blackberry Enterprise Server Version 4+ benötigen, müssen auf ScriptedGatewayResourceAdapter basieren.

Message-Queue

- JMS Message Queue Listener

Betriebssysteme

- HP OpenVMS 7.2
- HP-UX 11.0, 11i v1, 11i v2
- IBM AIX® 4.3.3, 5.2, 5L, v5.3
- IBM OS/400® V4r3, V4r5, V5r1, V5r2, V5r3, V5r4
- Microsoft Windows® NT® 4.0
- Microsoft Windows® 2000, 2003
- Generic UNIX Shell Script
- Generic Windows Script Adapter (verwendet Gateway)
- Red Hat Linux 8.0, 9.0
- Red Hat Linux Advanced Server 2.1
- Red Hat Linux Enterprise Server 3.0, 4.0
- Sun Solaris™ 8, 9, 10
- SuSE Enterprise 9

Rollenmanagement

- BridgeStream SmartRoles

Sicherheitsmanager

- ActivCard® 5.0
- eTrust CA-ACF2® Security
- Natural
- IBM RACF®
- Scripted Host
- INISafe Nexess 1.1.5
- RSA ClearTrust 5.5.2, 5.5.3
- RSA® SecurID® 5.0, 6.0
- RSA® SecurID® 5.1, 6.0 für UNIX
- eTrust CA-Top Secret® Security 5.3

Steuerung des Webzugriffs

- IBM Tivoli® Access Manager 4.*x*, 5.1
- Netegrity® Siteminder® 5.5
- RSA® ClearTrust® 5.0.1
- Sun™ ONE Identity Server 6.0, 6.1, 6.2
- Sun™ Java System Identity Server 2004Q2
- Sun™ Java System Access Manager 6 2005Q1, 7 2005Q4 (Realms werden ab 2005Q4 unterstützt)

Webserver

HINWEIS Die Integration zwischen einem Anwendungsserver und Webserver ist für Identity Manager nicht erforderlich. Die Auswahl eines Webservers bietet einen besseren Lastenausgleich und eine erhöhte Sicherheit (über das HTTPS-Protokoll).

- Apache 1.3.19
- iPlanet 4.1
- Microsoft Internet Information Server (IIS) 4.0, 5.0
- Sun™ ONE Web Server 6

Nicht mehr unterstützte Software

Identity Manager unterstützt in Zukunft folgende, als Anwendungsserver, Datenbank-Repositorys und verwaltete Ressourcen verwendete Softwarepakete nicht mehr. Die Unterstützung wird nur bis zur nächsten Hauptversion von Identity Manager fortgeführt. Wenden Sie sich bei Fragen zu neueren Versionen dieser Softwarepakete an Ihren Kundendienstmitarbeiter.

Softwarekategorie	Software-Package
Betriebssysteme	• IBM AIX 4.3.3 • Microsoft Windows NT 4.0
Anwendungsserver	• Apache Tomcat 4.1.x • Sun ONE Application Server 7
Repository-Datenbankserver	• MySQL 4.1
Ressourcen	• ActivCard 5.0 • Lotus Notes (Domino) 5.0 • Microsoft Exchange 5.5 • Microsoft Windows NT 4.0 • MySQL 4.1 • Red Hat Linux 8.0 • SAP R/3 v4.5, v4.6 • Siebel 6.2 • Sun ONE Identity Server 6.0

Die folgenden abhängigen Softwarepakete werden in Identity Manager 7.0 nicht mehr unterstützt

Softwarekategorie	Software-Package
Datenbankserver	• Oracle 8*i* • IBM DB2 Universal Database for Linux, UNIX, und Windows 7.0
Betriebssysteme	• Solaris 7 • IBM DB2 Universal Database for Linux, UNIX, und Windows 7.0
Ressourcen	• Microsoft Exchange 5.5 • IBM DB2 7.0

Offizieller Support für den NT4-Ressourcenadapter

Da in unseren letzten Versionen stets neue und verbesserte Funktionen implementiert wurden, wird die Unterstützung älterer Versionen in Zukunft eingestellt. Die Pläne für die Einstellung der Unterstützung beruhen darauf, dass Microsoft das Betriebssystem NT 4.0 nicht mehr unterstützt. Sun stellt die Unterstützung von Windows NT ein, die NT-Adapterfunktionalität wird jedoch weiterhin unterstützt. Kunden, die Windows NT verwenden, erhalten noch bis Ende 2006 Support zu diesem Betriebssystem.

API-Unterstützung

Die Identity Manager 7.0-Schnittstelle für die Anwendungsprogrammierung (API) enthält die folgenden, in der folgenden Tabelle aufgeführten öffentlichen Klassen (und öffentliche oder geschützte Methoden bzw. Felder öffentlicher Klassen):

API-Typ	Klassennamen
Sitzung	com.waveset.msgcat.*
	com.waveset.util.*
	com.waveset.object.*
	com.waveset.exception.*
	com.waveset.expression.*
	com.waveset.config.*
	com.waveset.session.SessionUtil
	com.waveset.session.ScriptSession
	com.waveset.session.SessionFactory
	com.waveset.session.Session
	com.waveset.session.UserViewConstants
Adapter	com.waveset.adapter.*
	com.waveset.util.Trace
Richtlinie	com.waveset.policy.PolicyImplementation
	com.waveset.policy.StringQualityPolicy
Bericht	com.waveset.report.BaseReportTask
Aufgabe	com.waveset.task.Executor
	com.waveset.task.TaskContext
UI	com.waveset.ui.FormUtil
	com.waveset.ui.util.RequestState
	com.waveset.ui.util.html.*
Workflow	com.waveset.provision.WorkflowServices
	com.waveset.session.WorkflowServices
	com.waveset.workflow.WorkflowApplication
	com.waveset.workflow.WorkflowContext

Identity Manager SPE enthält außerdem die in der folgenden Tabelle aufgeführten öffentlichen Klassen.

API-Typ	Klassennamen
SPE	com.sun.idm.idmx.api.*
	com.sun.idm.idmx.txn.TransactionPersistentStore
	com.sun.idm.idmx.txn.TransactionQuery
	com.sun.idm.idmx.txn.TransactionSummary

Diese Klassen sind die einzigen Klassen, die offiziell unterstützt werden. Wenn Sie Klassen verwenden, die in diesen Tabellen nicht aufgeführt sind, sollten Sie sich beim Kundendienst erkundigen, ob eine Migration zu einer unterstützten Klasse erforderlich ist.

Verworfene APIs

Der Abschnitt Verworfene APIs in diesen Versionshinweisen enthält alle Identity Manager-APIs, die in dieser Version verworfen wurden, und deren Nachfolger (falls verfügbar).

Aufrüstungsmöglichkeiten und Ende der Gültigkeitsdauer

Dieser Abschnitt enthält Informationen zu Aufrüstungsmöglichkeiten für Identity Manager und erläutert die Richtlinien für das Ende der Gültigkeitsdauer (End of Service Life, EOSL) für den Software-Support von Identity Manager.

Aufrüstungsmöglichkeiten für Identity Manager

Wählen Sie aus der folgenden Tabelle ein Verfahren aus, das Sie beim Aufrüsten auf eine neuere Version von Identity Manager verwenden sollten.

	Zielversion			
Aktuelle Version	**5.0**	**2005Q3M1**	**2005Q4M3**	**7.0**
Waveset Lighthouse 4.1 SP*x*	5.0	5.0 > 2005Q3M1	5.0 > 2005Q4M3	5.0 > 2005Q4M3 > 7.0
Identity Manager 5.0 SP*x*		2005Q3M1	2005Q4M3	2005Q4M3 > 7.0
Identity Manager 2005Q1M3 Identity Auditor 1.0		2005Q3M1	2005Q4M3	2005Q4M3 > 7.0
Identity Manager 2005Q3M1 Identity Manager 5.5			2005Q4M3	2005Q4M3 > 7.0
Identity Manager 2005Q3M3 Identity Manager SPE 1.0			2005Q4M3	2005Q4M3 > 7.0
Identity Manager 2005Q4M3 Identity Manager 6.0				7.0

HINWEIS

- Beim Aufrüsten von Identity Manager müssen Sie keine Service Packs der vorherigen Hauptversion installieren, um auf die nächsthöhere Hauptversion aufzurüsten Wenn Sie beispielsweise von Identity Manager 5.0 auf 6.0 aufrüsten, brauchen Sie keine Service Packs für Version 5.0 zu installieren.
- Service Packs für Hauptversionen sind kumulativ. Nach dem Aufrüsten auf die neue Hauptversion brauchen Sie nur das neueste Service Pack und nicht die vorherigen Service Packs für diese Version zu installieren. Wenn Sie beispielsweise auf Identity Manager 5.0 aufgerüstet haben, macht die Installation von SP6 die von SP1 bis SP5 bereitgestellte Funktionalität verfügbar.

Aktualisierungen für die Dokumentation von Identity Manager werden wie folgt bereitgestellt:

- **Jede Version** (einschließl. Service Packs): In den Versionshinweisen werden behobene Probleme, Produkterweiterungen, neue Funktionen und andere wichtige Informationen beschrieben.
- **Hauptversionen** (*x*.0): Das gesamte Dokumentationspaket von Identity Manager wird aktualisiert und neu veröffentlicht.
- **Zwischenversionen und Service Packs**: Einzelne Publikationen werden aktualisiert und neu veröffentlicht, oder es werden Dokumentationsergänzungen bereitgestellt.

Ende der Gültigkeitsdauer für den Software-Support

Vor dem Ende der Gültigkeitsdauer (End of Service Life, EOSL) von Identity Manager wird Software-Support in zwei Phasen angeboten:

- *Phase 1: Vollständiger Support*
- *Phase 2: Beschränkter Support*

HINWEIS Die Zeitdauer des vollständigen Supports ist je nach Produkt verschieden.

Vollständige Support-Phase

Während der vollständigen Support-Phase stellt Sun Microsystems, Inc. Software-Support gemäß dem zwischen dem Kunden und Sun abgeschlossenen Support-Vertrag (einschließlich geltender Service-Aufstellungen) bereit. Siehe:

http://www.sun.com/service/servicelist/

Wenn für ein Softwareprodukt jedoch das Ende der Gültigkeitsdauer bekanntgegeben wird, haben Kunden für dieses Softwareprodukt keinen Zugang mehr zu Aktualisierungen und Aufrüstungen.

Beschränkte Support-Phase

Während der beschränkten Support-Phase stellt Sun Microsystems, Inc. Software-Support gemäß dem zwischen dem Kunden und Sun abgeschlossenen Support-Vertrag (einschließlich geltender Service-Aufstellungen) bereit. Siehe:

http://www.sun.com/service/servicelist/

Kunden haben jedoch keinen Anspruch auf das Einsenden von Problemberichten und den Erhalt neuer Patches von Sun Microsystems, Inc. Wie beim vollständigen Support auch haben Kunden für dieses Softwareprodukt keinen Zugang mehr zu Aktualisierungen und Aufrüstungen, wenn für ein Softwareprodukt das Ende der Gültigkeitsdauer bekanntgegeben wird.

Die folgende Tabelle enthält die Enddaten der Gültigkeitsdauer (EOSL und EOL) für ältere Versionen von Identity Manager.

Produktname	Produktstatus	Letzte Auslieferung	Phase 1: Enddatum	Phase 2: Enddatum (EOSL)	Ankündigung des Endes der Gültigkeitsdauer
Sun Java System Identity Manager 6.0 2005Q4		05/25/2007	05/25/2008	05/2012	11/20/06
Sun Java System Identity Auditor 1.0 2005Q1	Post-RR	02/02/2007	02/2008	02/2012	08/01/06
Sun Java System Identity Manager Service Provider Edition 1.0 2005Q3	Post-RR	02/02/2007	02/2008	02/2012	08/01/06
Sun Java System Identity Manager 5.0 2004Q3	EOL	08/11/2006	08/2007	08/2011	02/07/06
Sun Java System Identity Manager 5.0 SP*x* 2004Q3	EOL	08/11/2006	08/2007	08/2011	02/07/06
Sun Java System Identity Manager 5.5	EOL	08/11/2006	08/2007	08/2011	02/07/06
Waveset Lighthouse 4.1			03/2006	03/2010	

Dateien zur freien Weitergabe

Sun Java System Identity Manager 7.0 enthält keine Dateien zur freien Weitergabe.

Melden von Problemen und Einsenden von Hinweisen und Vorschlägen

Wenn Sie mit Sun Java System Identity Manager Probleme haben, können Sie sich mit dem Sun-Kundendienst unter einem der folgenden Kanäle in Verbindung setzen:

- Sun Software Support online unter
  `http://www.sun.com/service/sunone/software`

  Auf dieser Seite finden Sie Links zur Wissensbasis (Knowledge Base), zum Online Support Center und zum ProductTracker sowie Links zu Wartungsprogrammen und Kontaktdetails für Supportverträge.

- Die auf Ihrem Wartungsvertrag angegebene Telefonnummer

Halten Sie folgende Informationen bereit, wenn Sie sich mit dem Technischen Support in Verbindung setzen, damit wir Ihnen bei der Lösung Ihres Problems schnellstmöglich behilflich sein können:

- Beschreibung des Problems einschließlich Bedingungen, unter denen es auftritt, und die Auswirkung auf innerbetriebliche Abläufe
- Rechnertyp, Betriebssystem- und Produktversion einschließlich Patches oder anderer Softwarepakete, in deren Zusammenhang das Problem auftritt
- Ausführliche Schritte zum Verfahren, mit dem Sie das Problem simulieren können
- Eventuelle Fehlerprotokolle und Speicherabzüge

Sun freut sich über Ihre Meinung

Sun ist stets an einer Verbesserung der eigenen Dokumentation interessiert und nimmt Ihre Kommentare und Anregungen gerne entgegen.

Gehen Sie zu http://docs.sun.com und klicken Sie auf „Kommentare senden". Geben Sie auf dem Online-Formular den Dokumenttitel und die Bestellnummer an. Die Bestellnummer ist sieben- bzw. neunstellig und befindet sich oben auf der Titelseite eines Dokuments. Der Titel dieses Dokuments ist beispielsweise Sun Java System Identity Manager November 2006 Versionshinweise, und die Teilenummer ist 820-0158-10.

Weitere Sun-Ressourcen

Nützliche Informationen zu Sun Java System finden Sie unter den folgenden Internetadressen:

- Dokumentation für Sun Java™ System Identity Manager
  http://docs.sun.com/app/docs/coll/1514.1
- Sun Java SystemDokumentation
  http://docs.sun.com/prod/java.sys
- Dienstleistungen für Sun Java System
  http://www.sun.com/service/sunps/sunone
- Sun Java System Softwareprodukte und Service
  http://www.sun.com/software
- Dienstleistungen zum Software-Support von Sun Java System
  http://www.sun.com/service/sunone/software
- Sun Java System Support und Knowledge Base (Wissensbasis)
  http://www.sun.com/service/support/software
- Sun-Support und -Schulung
  http://training.sun.com
- Consulting und Dienstleistungen für Sun Java System
  http://www.sun.com/service/sunps/sunone
- Sun Java System - Informationen für Entwickler
  http://developers.sun.com

- Sun Developer Support Services
  http://www.sun.com/developers/support
- Softwareschulung für Sun Java System
  http://www.sun.com/software/training
- Sun Softwaredatenblätter
  http://www.sun.com/software

Identity Manager 7.0-Funktionen

Neue Funktionen in dieser Version

Sun Identity Manager 7.0 integriert die drei Softwareprodukte Identity Manager, Identity Manager SPE sowie Identity Auditor in ein einziges Paket namens Sun Java System Identity Manager 7.0. Diese integrierte Lösung ist ein konsistentes und skalierbares Hilfsmittel zur Identitätskontrolle für Provisioning- und Überprüfungsprozesse.

Weitere neue Leistungsmerkmale:

- Erweiterte Auditor-Funktionen einschließl.
    - Unterstützung für regelmäßige Zugriffsprüfungen
    - Zusammenfassende und ausführliche Aufgabentrennungsberichte
    - Erweiterte Schnittstelle mit Zugriff durch einen einzigen Mausklick auf Arbeitseinheiten für Korrekturen und Zugriffsprüfungen
- Sofort einsatzfähige Benutzeroberfläche einschließl.
    - Zugriff auf Arbeitselemente durch einen einzigen Mausklick
    - Registerkarten zur einfachen Navigation und benutzerspezifischen Anpassung
- Service Provider-Aktualisierungen:
    - Verzeichnisbasierte delegierte Administration
    - Unterstützung für Workflow-Legenden; und Benachrichtigungen
- Eine neue, auf NetBeans basierende integrierte Entwicklungsumgebung (Integrated Development Environment, IDE) für Identity Manager
- Zusätzliche Leistungsmerkmale:
    - Unterstützung für SPML 2.0
    - Metrikberichte mithilfe der Ereignisverfolgung

Im Abschnitt Zusammenfassung der Funktionen finden Sie zusätzliche Informationen zu neuen Leistungsmerkmalen von Identity Manager 7.0.

Zusammenfassung der Funktionen

In diesem Abschnitt finden Sie einen Überblick zu den neuen Leistungsmerkmalen von Identity Manager 7.0.

Installation und Aktualisierung

- Identity Manager unterstützt jetzt als Repository Oracle Database 10g Release2®. (ID-12908).
- `UserEntitlement`-Objekte werden jetzt in der Datenbank in einer eigenen Tabelle gespeichert. (ID-13612).

  Zum Aufrüsten einer vorhandenen Identity Manager-Installation ist das entsprechende Datenbankskript `upgradeto70.*` auszuführen, bevor diese Installation auf Identity Manager 7.0 aufgerüstet wird. Diese Skripten fügen die Datenbanktabellen hinzu, die zur Unterstützung von Identity Manager-Objekten zur regelmäßigen Zugriffsprüfungen erforderlich sind.
- Die Lizenzstruktur wurde aus dem Softwarepaket entfernt. Eine Aufrüstung auf Identity Manager 7.0 ist für alle Softwareprodukte voll funktionsfähig. Für Lizenzen gibt es keine Lizenzfenster bzw. Befehlszeilenoptionen mehr. Wenn Sie versuchen, dieses Produkt zu lizenzieren, wird der Fehler "command not found" (Befehl nicht gefunden) ausgegeben. (ID-13632 13501)

Administratorbenutzeroberfläche und Benutzeroberfläche

- Auf der Seite „Identity-Attribute" gibt es jetzt einen Passwortbereich, in dem der Status der Passworterstellung in Bezug auf Identity-Attribute beschrieben wird. Sie können Identity Manager so konfigurieren, dass Passwörter neuen Benutzern aufgrund eines Standardwertes (z.B. einer Regel) oder einer Identity System-Kontorichtlinie, die Passwörter erzeugt, zugewiesen werden. (ID-10274, 12560).
- Die Strukturtabellenkomponente unterstützt jetzt veränderliche Tabellenspaltenbreiten. Mit CSS können Sie die Spaltenbreiten der Benutzerliste und der Ressourcenlistentabellen auf einen absoluten Pixelwert oder einen Prozentsatz einstellen. Sie können darüber hinaus Tabellenspaltenbreiten mit der Maus durch Klicken und Ziehen der Begrenzung der entsprechenden Spaltenüberschrift ändern. (ID-11474).
- Der Inhalt von Strukturtabellen für Konten und Ressourcen kann jetzt sortiert werden. (ID-12086).
- Die Menühierarchie für die Endbenutzerseiten ist jetzt benutzerspezifisch anpassbar. (ID-12415).

- Identity Manager enthält jetzt das Standardattribut „Manager“, das eine Manager-Mitarbeiter-Beziehung unterstützt. Diese Information wird im Identity Manager-Benutzerobjekt gespeichert. (ID-12416).
- Fehler auf Seitenebene und Informationsmeldungen werden jetzt am oberen Seitenrand in einem Kasten mit Fehler- bzw. Informationssymbol angezeigt. Früher wurden solche Meldungen entweder mit rotem Text (bei Fehlern) oder einem kleinem Symbol für Informationsmeldungen angezeigt. (ID-12625).
- Benutzer können jetzt anfordern, dass Rollen und Ressourcen-Mitgliedschaften zugewiesen und entfernt werden. Manager können diese Funktion auch für unterstellte Mitarbeiter ausführen. (ID-13018).
- Sie können jetzt die Polarität der abwechselnd grau und weiß dargestellten Zeilen durch Hinzufügen der Eigenschaft `rowPolarity` zu EditForm-Komponenten in XPRESS ändern. Standardwert: „true“. Durch den Wert „false“ wird die Polarität umgekehrt und das erste Formularfeld mit weißem Hintergrund dargestellt. (ID-13971).
- Die Benutzeroberfläche unterstützt jetzt einen Selbsterkennungs-Link. Der Link “Identity System über andere Konten informieren” wurde aus der Endbenutzerstartseite entfernt und befindet sich jetzt auf der neuen Registerkarte „Selbsterkennung“ in der Navigationsleiste unter „Profil“. (ID-14698).
- In der folgenden Tabelle ist aufgeführt, wie Registerkartenhierarchien in dieser Version umgestaltet wurden:

Registerkarten in der vorherigen Version		Registerkarten in dieser Version		Kommentare
Genehmigungen		Arbeitseinheiten>	Genehmigungen	
			Eigene Arbeitseinheiten	Diese neue Registerkarte zeigt einen Überblick über alle Arbeitseinheiten und stellt den Ausgangspunkt zum Abarbeiten von Arbeitseinheiten dar.
			Bescheinigungen	Diese neue Registerkarte unterstützt das neue Leistungsmerkmal zu regelmäßigen Zugriffsprüfungen und ermöglicht das Abarbeiten von Bescheinigungsarbeitseinheiten.
			Sonstige	Auf dieser neuen Registerkarte können zugewiesene Arbeitseinheiten, bei denen es sich nicht um Genehmigungen, Bescheinigungen oder Korrekturen handelt, abgearbeitet werden.
			Verlauf	Diese Registerkarte zeigt einen Bericht aller von einem Benutzer durchgeführten Genehmigungen, Ablehnungen, Minderungen und Korrekturen an.
			Eigene Arbeitseinheiten delegieren	Mithilfe dieser Registerkarte können alle Arbeitseinheiten an einen anderen Benutzer delegiert werden.
		Konformität >	Richtlinien verwalten Zugriffsabfragen verwalten Zugriffsprüfung	Diese neuen Registerkarten dienen zum Einrichten und Verwalten von Zugriffsrichtlinien und Zugriffsprüfungen.
Konfigurieren >	Berichte	Berichte >	Konfigurieren	Diese Änderung macht den Zugriff auf Berichtsfunktionen klarer.
Konfigurieren >	Verwaltete Ressourcen	Ressourcen >	Typen konfigurieren	Diese Änderung macht die Zuordnung dieser Funktion zu Ressourcen klarer.
Konfigurieren >	Admin-Rollen Fähigkeiten Zertifikate Anmelden Richtlinien	Sicherheit >	Admin-Rollen Fähigkeiten Zertifikate Anmelden Richtlinien	Die Registerkarte „Sicherheit“ ist in dieser Version neu und dient zur klareren Gruppierung der Funktionen für sicheren Kontozugang und Zugriffsrechte.
Konfigurieren >	Metaansicht	Metaansicht >	Identity-Attribute Identity-Ereignisse	Mit dieser Registerkarte können Identity-Attribute und -Ereignisse direkt bearbeitet werden.

Registerkarten in der vorherigen Version		Registerkarten in dieser Version		Kommentare
Risikoanalyse >	Berichte ausführen Berichte verwalten	Berichte >	Risikoanalyse ausführen Risikoanalyse anzeigen	Diese Änderung fasst diese Bericht mit anderen Berichten zusammen.
Service Provider Edition	Bedienfeld-diagramme Bedienfelder anzeigen	Berichte >	Bedienfelddiagramme Bedienfelder anzeigen	Diese der Registerkarte „Berichte“ untergeordneten Registerkarten repräsentieren neue Funktionen aus der Service Provider Edition zum Anzeigen und Gruppieren grafischer Berichte.
Service Provider Edition		Konten	Service Provider-Benutzer verwalten	Mit dieser Registerkarte können Sie Benutzer vom Typ Service Provider in Identity Manager verwalten.
Service Provider Edition >	Transaktionen durchsuchen	Serveraufgaben	Service Provider-Transaktionen	Die Registerkarte „Transaktionen durchsuchen“ wurde aus der Registerkarte „Service Provider“ in der Service Provider Edition entfernt und befindet sich nun auf der Registerkarte „Service Provider-Transaktionen“ der Registerkarte „Serveraufgaben“.
Aufgaben		Serveraufgaben		Diese Registerkarte wurde umbenannt, um zu verdeutlichen, dass Aufgaben Prozesse sind, die auf dem Server ausgeführt werden.
Registerkartenänderungen von Identity Auditor zu Identity Manager 7.0				
Konformität >	Benutzer Richtlinienansicht Ressourcenansicht Organisations-ansicht	Konten	Menü „Benutzer-aktionen“	Alle Benutzeraktionen werden in Identity Manager von der Registerkarte „Konten“ aus ausgeführt. Die Registerkarten „Richtlinienansicht“, „Ressourcenansicht“ und „Organisationsansicht“ wurden entfernt; die entsprechenden Berichte sind jedoch noch in der Registerkarte „Berichte“ verfügbar. Die Aktionen „Protokoll der Konformitätsverletzungen anzeigen“ und „Konformitätsstatus anzeigen“ stehen jetzt unter „Benutzeraktionen“ zur Verfügung.
Steuerung >	Richtlinien verwalten	Konformität >	Richtlinien verwalten	

Registerkarten in der vorherigen Version		Registerkarten in dieser Version		Kommentare
Konfigurieren >	Richtlinien	Konten >	Menü „Benutzeraktionen“	Benutzerüberwachungsrichtlinien bearbeiten Organisationsüberwachungsrichtlinien bearbeiten
Korrekturen>	Korrekturen Ausstehend Abgeschlossen	Arbeitseinheiten>	Korrekturen Verlauf	Die Registerkarten „Ausstehend“ und „Abgeschlossen“ wurden entfernt. In der Registerkarte „Korrekturen“ werden noch ausstehende Korrekturen angezeigt. In der Registerkarte „Verlauf“ werden abgeschlossene Korrekturarbeitseinheiten angezeigt.
Berichte >	Berichte ausführen Berichte verwalten	Berichte >	Berichte ausführen Berichte anzeigen	Alle Auditor-Berichte sind jetzt in der Registerkarte „Berichte“ durch Auswahl des Typs „Auditor-Berichte“ abrufbar.
Aufgaben		Serveraufgaben		

Überprüfung

- Die Überprüfungsframeworks von Identity Manager und Identity Manager SPE wurden vereinigt. Dabei wurden folgende Änderungen vorgenommen: (ID-13148).
    - Identity Manager und Identity Manager SPE besitzen keine getrennten Frameworks zur Überprüfungsprotokollierung mehr.
    - Die Schnittstellen zur Überprüfungsprotokollierung von Identity Manager SPE wurden verworfen.
    - Mithilfe des vereinheitlichten Dienstes zur Überprüfungsprotokollierung können Dritte benutzerspezifische Überprüfungsherausgeber entwickeln, die Überprüfungsereignisse von Identity Manager und Identity Manager SPE behandeln.
    - Javadoc-Dokumentation der neuen öffentlichen Schnittstellen ist im Referenz-Kit verfügbar.
    - Beispielcode zum Demonstrieren des Frameworks zur Überprüfungsprotokollierung wurde zum Referenz-Kit hinzugefügt.

Auditor

Mithilfe regelmäßiger Zugriffsprüfungen kann das Sammeln und Bescheinigen von aktuellen Benutzerzugriffsrechten auf kritische Systeme und Anwendungsprogramme automatisiert werden. Diese Funktion ermöglicht das Erstellen von Einträgen, die den Zugriffsstatus enthalten, den ein Benutzer auf ein oder mehrere Systeme bzw. Anwendungsprogramme hat. Jedem dieser Einträge kann automatisch das Einhalten der Richtlinienregeln bescheinigt werden, oder er kann zum Ausstellen einer manuellen Bescheinigung an eine zuständige Person weitergeleitet werden. (ID-9719).

Zugriffsprüfungen werden normalerweise regelmäßig durchgeführt, um sicherzustellen, dass Benutzer keinen übermäßigen Zugriff auf kritische Systeme besitzen. Durch Speichern von Benutzerzugriffsdaten für mehrere Systeme und Anwendungsprogramme in einem einzigen Eintrag können sich Personen, die Zugriffsprüfungen auswerten, ein vollständiges Bild vom Zugriffsprofil eines Benutzers machen, was wiederum die Beurteilung dieser Rechte erleichtert. Der automatisierte Prozess wird durch Verfolgungstools unterstützt, die angeben, wie viel von einer Zugriffsprüfung abgearbeitet wurde, wie viel noch abzuarbeiten ist, und wer für die verbleibenden Arbeiten verantwortlich ist. Dieser Auswertungsprozess ist so in herkömmlichen Überprüfungsrichtlinienabfragen integriert, dass dabei sowohl Konformitätsprüfungen (Überprüfungsrichtlinienabfragen) und Zugriffsprüfungen (Berichtserstellung und Bescheinigung) ausgeführt werden können.

Zur weiteren Automatisierung können Zugriffsprüfungen benutzerspezifisch angepasst werden, u.a. durch:

- Regelbasierte Entscheidung, ob Benutzer Bescheinigungen ausgestellt bekommen oder nicht
- Regelbasierte Entscheidung, ob Bescheinigungen/Ablehnungen für Benutzer automatisch ausgestellt werden oder nicht
- Regelbasierte Entscheidung, welche Person für Benutzer manuell Bescheinigungen ausstellen soll
- Workflow-basierte manuelle Bescheinigung einschließl. Weiterleitung, Delegierung und zusätzlicher Genehmigung
- Bescheiniger müssen keine IdM-Administratoren sein, beliebige IdM-Konten reichen dafür aus

Eine weitere neue Funktion im Auditor-Modul sind Aufgabentrennungsberichte. Damit werden spezifische Zugriffskonflikte erkannt, mit denen Benutzer interne Schutzmechanismen umgehen können. (ID-12716) Solche Konflikte wirken sich besonders in ERP- und Finanzsystemen aus, wo eine Verletzung von Zugriffsregeln finanzielle Fehler nach sich ziehen kann. Das Auditor-Modul erkennt solche Konflikte mithilfe eines Verstoßeintrags, der den Benutzernamen, das betroffene System/Anwendungsprogramm, den spezifischen Konflikt sowie die genauen Konteneinstellungen, die den Konflikt verursachen, enthält. Auditor- Aufgabentrennungen erkennen Konflikte mit Konteneinstellungen entweder in einem einzigen System/Anwendungsprogramm oder über mehrere Systeme hinweg.

Diese Konflikte werden in einem Konflikt-Matrixbericht zusammengefasst. Ausführliche Informationen sind dann über die einzelnen Matrixzellen abrufbar.

Formulare

- MultiSelect unterstützt jetzt die neue Eigenschaft `displayCase`, die auf “upper” oder “lower” gesetzt werden kann. Diese Funktion entspricht der Definition einer `valueMap`, die jedem der `allowedValues` (zulässigen Werte) einen entsprechenden Text in Groß- bzw. Kleinschreibung zuordnet. (ID-8356).

HTML-Anzeigekomponenten

- Die Komponente `SortingTable` unterstützt jetzt die Eigenschaften „align“, „valign“ und „width“ der untergeordneten Komponenten, die bei der HTML-Ausgabe die jeweilige Tabelle enthalten. Zur Anzeige von Fehlermeldungen, Warnhinweisen und Informationsmeldungen in Formularen steht darüber hinaus die `InlineAlert` -Komponente zur Verfügung. (ID-12560).

Integrierte Entwicklungsumgebung von Identity Manager (Integrated Development Environment, IDE)

Die Identity Manager Integrated Development Environment (Identity Manager IDE) ist eine Java-Anwendung, mit der Sie Identity Manager-Objekte in Ihrer Bereitstellung anzeigen und anpassen sowie darin Fehler suchen können.

Zu den wichtigsten Funktionen der Identity Manager IDE gehören:

- Integriertes Explorer-Fenster zur projekt-, verzeichnis- oder laufzeitbasierten Ansicht eines Projektes
- Aktionsmenüs zur Dokumentationsänderung
- Benutzerspezifisch anpassbare Editoren, z.B.:
  - Arbeitsblätter zu Objekteigenschaften und grafische Editoren zum Auflisten von XML-Objekteigenschaften und Bearbeiten von grundlegenden Objekttypen sowie XPRESS- und XML-Objekten, ohne XML-Code eingeben zu müssen
  - Drag-and-Drop-Palette zum Hinzufügen von Workflow-Diensten, Genehmigungen, Benutzern und Workflow-Aufgaben zu XML-Quellcode, ohne XML-Code eingeben zu müssen
  - Registrierte Definitionsdatei `waveset.dtd`, die das Hervorheben von XML-Syntax und automatische Vervollständigen von XML-Elementen und Attributen ermöglicht
- Integrierter Debugger für Workflows, Formulare und Regeln
- Regeltester zum Überprüfen eigenständiger und in Bibliotheken enthaltener Regeln
- Formularvorschau zum Anzeigen von und Suchen von Fehlern in Formularen in einem externen Browser
- Die Funktion „Ansicht auschecken" ermöglicht Ihnen, Identity Manager-Ansichten wie z.B. Benutzeransichten auszuchecken, zu ändern und wieder einzuchecken.
- CVS-Integration

Die Identity Manager IDE ist ein vollständig integriertes NetBeans-Plugin und löst den Business Process Editor (BPE) von Identity Manager ab. Weitere Information zur Installation und Verwendung der Identity Manager IDE finden Sie im Kapitel „Using the Identity Manager IDE" in *Identity Manager Deployment Tools*.

Identity Manager SPE

- Identity Manager SPE-Daten zur Konfiguration und Ereignisverfolgung werden nicht mehr auf einem LDAP-Verzeichnisserver gespeichert. (ID-12170).

  Identity Manager SPE-Komponenten lesen diese Daten jetzt direkt aus dem Repository von Identity Manager. Deswegen müssen die für Identity Manager SPE erforderlichen Konfigurationsobjekte nicht mehr ausgewählt und exportiert werden. Ein bereits vorhandenes Identity Manager SPE-Deployment kann mithilfe des Identity Manager-Installationsprogramms aktualisiert werden.

  Falls Daten zur Ereignisverfolgung im Konfigurationsverzeichnis von Identity Manager SPE gespeichert sind, sollten diese vor der Aufrüstung im XML-Format exportiert werden. Nach der Aufrüstung können die Daten zur Ereignisverfolgung in Identity Manager importiert werden. Nach dem erfolgreichen Abschluss einer Aufrüstung kann das LDAP-Konfigurationsverzeichnis dann sicher gelöscht werden.

- Für den Zugriff auf Objekte mit Identity Manager SPE ist kein eigener Kontexttyp mehr erforderlich. In Identity Manager SPE-Formularen braucht die Eigenschaft `needSpeContext` nicht mehr gesetzt zu werden und dieser Kontext muss nicht mehr mithilfe von `:display.speContext` referenziert werden. (ID-12171).

- Es wurde eine öffentliche Schnittstelle erstellt, die es Kunden ermöglicht, vor und nach dem Provisioning benutzerdefinierte Zusatzaktionen aufzurufen. (ID-12173).

- Identity Manager SPE bietet jetzt bessere JSP-Beispiel- und Endbenutzerseiten. (ID-12175).

- Identity Manager bietet jetzt ein benutzerspezifisch anpassbares Modell zur delegierten Administration und Autorisierung, das sowohl von Identity Manager und Identity Manager SPE User Server aus zugänglich ist. Dieses Modell baut auf Verzeichnisattributen auf und ist nicht von Identity Manager-Organisationen und -Fähigkeiten abhängig. (ID-12176).

- Active Sync- und SPE-Synchronisierungen sind jetzt auf dem gleichen Identity Manager-Server ausführbar, dürfen jedoch nicht auf der gleichen Ressource ausgeführt werden. (ID-12178).

- Das Identity Manager SPE-Attribut „User XML" ist jetzt im komprimierten Format speicherbar, um den Speicherplatzbedarf des SPE-Benutzerverzeichnisses zu verringern. (ID-12186).

- Identity Manager SPE-Transaktionen unterstützen jetzt konfigurierbare Konsistenzebenen zur Benutzeraktualisierung. Vorhandene Transaktionsdatenbanken müssen um eine zusätzliche Spalte (`userId VARCHAR(N)`) erweitert werden, wobei `N` groß genug sein muss, um die erwartete Maximallänge eines Identity Manager SPE Benutzer-DNs plus zusätzlich 8 Zeichen enthalten zu können. Diese Datenbankänderung wird beim Ausführen der Aufrüstungsskripten nicht automatisch vorgenommen. (ID-13830).

MetaView

- MetaView wurde um die neue Funktion „Identity-Ereignisse“ erweitert. Mit dieser Option können Sie ein Modell entwickeln, das erkennt, wenn Ereignisse auf Ressourcen auftreten, und wie beim Auftreten solcher Ereignisse reagiert werden soll. Mit dieser Funktion können Sie darüber hinaus Ereignisse entweder direkt in der betreffenden Ressource oder durch Auswertung einer Regel (wenn die betreffende Ressource die Ereigniserkennung nicht unterstützt) löschen, deaktivieren und aktivieren.

  Sie können auf Ereignisse mit beliebigen Kombinationen des Löschens, Zurücksetzens von Zuweisungen und Verknüpfungen, Aktivierens und Deaktivierens von Benutzern bzw. Ressourcenkonten reagieren. Identity-Ereignisse werden nur während Active Sync-Phasen angewendet. Wie bei Identity-Attributen auch werden diese Ereignisse nur dann angewendet, wenn Active Sync für MetaView aktiviert wurde. (ID-12561).
- Die Administratorschnittstelle wurde um die Funktion „Berichte gelöscht“ erweitert. Diese Funktion gilt für Ressourcenadapter, die Active Sync direkt unterstützen und erkennen können, ob Konten gelöscht wurden. (ID-13206).
- MetaView unterstützt jetzt eine neue Option zum Setzen der Werte von Zielfeldern. Attribute mit mehreren Werten können darüber hinaus zusammengeführt werden. (ID-13212).

Berichte

- Ergebnisse von Massenaktionen können jetzt in eine Datei im CSV-Format exportiert werden. (ID-9297).
- Der Gültigkeitsbereich der folgenden Berichtstypen wird standardmäßig auf die vom angemeldeten Administrator kontrollierten Organisationen abgestimmt, es sei denn, es wurden explizit eine oder mehrere Organisationen ausgewählt, für die der betreffende Bericht gelten soll: „Admin-Rolle - Zusammenfassung“, „Administrator - Zusammenfassung“, „Rollen - Zusammenfassung“, „Benutzerfragen - Zusammenfassung“ und „Benutzer - Zusammenfassung“. Die Gültigkeitsbereichskomponente `org` wurde ebenfalls von einer Einfach- in eine Mehrfachauswahlkomponente umgewandelt. (ID-12116).
- Identity Manager unterstützt jetzt die Überwachung einer Reihe von Komponenten mithilfe von Java Management Extensions (JMX). (ID-12405).
- Die folgenden neuen Berichtstypen unterstützen jetzt Manager-Mitarbeiter-Beziehungen: „Eigene direkte Berichte - Zusammenfassung“, „My Direct Employee Summary“, „My Direct and Indirect Employee Summary“ und „My Direct Reports Individual“. (ID-12416, ID-12689).
- CSV-Berichte mit UTF-8-Zeichensatz und Multibyte-Text sind jetzt entsprechend anpassbar, sodass sie von Anwendungsprogrammen, die den UTF-8-Zeichensatz nicht unterstützen (wie z.B. Microsoft Excel), angezeigt werden können. (ID-13574).

Repository

- Administratoren können das automatische interne Verbindungs-Pooling des Identity Manager-Repository durch Setzen des Attributs `connectionPoolDisable` des Objektes `RepositoryConfiguration` auf „true" deaktivieren. Die frühere Methode des Setzens von `com.waveset.repository.ConnectionPoolDisable=true` wurde verworfen. (ID-10924).
- Identity Manager 7.0 entfernt die Repository-Methodensignatur `#getLastMod(Type, long)`. In Identity Manager 5.0 SP2 wurde diese Methodensignatur von `#getLastMod(Type)` abgelöst. Benutzerdefinierte Anwendungen dürfen diese Methode nicht aufrufen. Darüber hinaus dürfen auch keine Klassen bzw. Interfaces aus dem Package `com.waveset.repository` mehr referenziert werden. (ID-11761).
- Der JDBC-Standardtreiber für Microsoft SQL Server ist jetzt der Microsoft SQL Server 2005 JDBC-Treiber. Dieser Treiber löst den älteren Microsoft SQL Server 2000 JDBC-Treiber ab. Durch diesen neuen Standardtreiber ändern sich der Name der JDBC-Treiberklasse und das Format der SQL Server Datenbank-URLs. An solche URLs braucht darüber hinaus kein Parameter "`SelectMethod=Cursor`" mehr angefügt zu werden. (ID-14136).

Ressourcen

- Identity Manager 7.0 unterstützt die folgenden Ressourcen:
    - Skript-JDBC (ID-7540)
    - BridgeStream SmartRoles (ID-12262)
    - Realm-Unterstützung in Sun Java System Access Manager (ID-12414)
- SecurId-Adapter können jetzt Token nach Status abrufen (z.B. alle Token mit dem Status LOST oder ENABLED). (ID-7646).
- Unterstützung für OS/400 v4r5, v5r2, v5r3 und v5r4 (5.2, 5.3 und 5.4) ist jetzt vorhanden. (ID-9928, 13122).
- Der Oracle ERP-Adapter wurde zur Unterstützung von Überprüfungsfunktionen um mehrere Attribute erweitert. (ID-11725).
- Der RACF-Adapter unterstützt jetzt Suchfilter für `listAllObjects`. (ID-10895).
- Der SAP HR Active Sync-Adapter unterstützt jetzt mySAP ERP ECC 5.0 (SAP 5.0). (ID-12408).

- Die SAP- und SAPHR-Adapter enthalten jetzt drei neue Ressourcenattribute, die Parameter zum Wiederholen einer SAP-Operation nach Netzwerkfehlern verfügbar machen: (ID-12579).
  - SAP-BAPI-Wiederholungen: gibt an, wie oft der betreffende Vorgang wiederholt werden soll.
  - SAP-Verbindungswiederholungen: gibt an, wie oft der Versuch der Verbindungsherstellung zum SAP-Server wiederholt werden soll.
  - Intervall für SAP-Verbindungswiederholungen: gibt an, wie lange (in ms) gewartet werden soll, bis der Versuch der Verbindungsherstellung zum SAP-Server wiederholt werden soll.
- Der Oracle ERP-Adapter unterstützt jetzt die Set-of-Books-Funktionalität (SOB). (ID-12715).
- Eine VLV-Sortierung ist jetzt konfigurierbar. Die LDAP-Ressource wurde um das VLV-Sortierungsattribut (`vlvSortAttribute`) erweitert. Wenn dieses Attribut gesetzt ist, wird dieser Wert für die Sortierung verwendet. Ist es nicht gesetzt, wird der Wert “`uid`” verwendet. (ID-13321).

Rollen

- Mithilfe von Rollen und Ressourcengruppen können Benutzern jetzt einzeln oder in Kombinationen auf einer Ressource mehrere Konten zugewiesen werden. (ID-6684).

Sicherheit

- Benutzer mit der Berechtigung „Genehmiger“ können alle zukünftigen Genehmigungsanforderungen für einen bestimmten Zeitraum an einen oder mehrere Benutzer, die keine Identity Manager-Genehmiger sind, delegieren. Die Delegierung ist mithilfe dreier Methoden möglich: (ID-8485).
  - Endbenutzer-Hauptmenü: Link „Genehmigungen delegieren“
  - Registerkarte „Genehmigungen“: Untergeordnete Registerkarte „Eigene Genehmigungen delegieren“
  - Admin - Benutzerkonto erstellen/bearbeiten/anzeigen Abschnitt „Sicherheit“

Server

- Identity Manager 7.0 unterstützt jetzt JBoss Application Server. (ID-10620).
- Identity Manager 7.0 kann jetzt eine große Anzahl ähnlicher Ressourcen erstellen und verwalten. (ID-11325).

SOAP

- Identity Manager 7.0 unterstützt jetzt die Service Provisioning Markup Language Version 2.0 (SPML). (ID-12417).

Workflow

- Arbeitseinheiten können jetzt von jedem beliebigen Benutzer delegiert werden. Diese Option ist sowohl auf der Administratoroberfläche als auch auf der neuen Endbenutzeroberfläche konfigurierbar. (ID-14110).

Probleme, die in dieser Version behoben wurden

In diesem Abschnitt werden die in Identity Manager 7.0 behobenen Probleme beschrieben.

Installation und Aktualisierung

- Anmeldedaten können jetzt an `com.waveset.install.UpgradePostProcess` übergeben werden. Diese Änderung erleichtert die Aktualisierung besonders dann, wenn das Konfiguratorpasswort geändert wurde und eine manuelle Aufrüstung ohne verfügbare grafische Benutzeroberfläche durchgeführt wird. (ID-13006).
- Der Schnittstelle zur Auditor-Anmeldung wurde entfernt. (ID-14481).

  Vor dem Aufrüsten sind folgende Aspekte zu berücksichtigen:

  - Vorhandene Kontenrichtlinien, die Fragen für das Auditor-Modul enthalten, werden wie folgt geändert:
    - Wenn die betreffende Richtlinie auch Fragen für das Admin-Modul und/oder die Standardanwendung enthält, werden die Fragen für das Auditor-Modul verworfen und stattdessen die Fragen für das Admin-Modul bzw. die Standardanwendung berücksichtigt.
    - Wenn die betreffende Richtlinie keine Fragen für das Admin-Modul und/oder die Standardanwendung enthält, werden die Fragen für das Auditor-Modul für das Admin-Modul verwendet.

  - Authentifizierungsantworten für Benutzer, die vom Auditor-Modul definiert wurden, werden wie folgt geändert:
    - Wenn die Benutzerdefinition auch Antworten für das Admin-Modul und/oder die Standardanwendung enthält, werden die Fragen für das Auditor-Modul verworfen.
    - Wenn die Benutzerdefinition keine Antworten für das Admin-Modul oder die Standardanwendung enthält, werden die Antworten für das Auditor-Modul für das Admin-Modul verwendet.
- Nach Aufrüstungen von einer früheren Installation, in der Identity Auditor aktiviert war, erscheint jetzt in der Konten-/Organisationstabelle die Organisation „Auditor". Neuinstallationen enthalten keine Organisation „Auditor". (ID-14636).
- Wenn Sie in einer früheren Version eine Überprüfungsrichtlinienregel für eine Pflichtentrennung erstellt haben, die das Anpassen des Formulars „Details zum Richtlinienverstoß" erforderlich machen, müssen Sie dieses Formular vor dem Aufrüsten speichern. (ID-14772).

Administratorbenutzeroberfläche und Benutzeroberflächen

- Wenn ein Benutzer versucht, sich an einer Ressource anzumelden, die nicht in Betrieb ist, wird eine hilfreiche Fehlermeldung angezeigt. (ID-1905).
- Meldungen für Fehler, die als kritisch gelten, können jetzt mit einer konfigurierten Standardmeldung angezeigt werden, und zusätzliche Informationen sind in `syslog` protokollierbar. Die UNIX-Ressourcenadapter wurden entsprechend geändert, damit sie diese Fehlermeldungsanzeige nutzen können. (ID-5495).
- Der Produktname in der Titelleiste des Browsers kann jetzt durch einen lokalisierbaren Text Ihrer Wahl ersetzt werden. (ID-10905).
- Die Aufgabe „Completed Role Synchronization" zeigt keine Meldung mehr an, die darauf hinweist, dass die Aufgabe noch ausgeführt wird. Diese Aufgabe wurde auch um eine Statistiktabelle erweitert. Für die abgeschlossene Aufgabe werden jetzt Fehler und Ausnahmefehler angezeigt. (ID-11181).
- Die Endbenutzerseite "Antworten auf Authentifizierungsfragen ändern" behandelt jetzt Benutzer, die keine Authentifizierungsfragen haben, sorgfältiger. (ID-11773).
- Der Link im Anmeldefenster für eine anonyme Benutzeranmeldung zeigt jetzt auf die neue Endbenutzer-Arbeitseinheitentabelle. (ID-12816).
- MultiSelect-Objekte sortieren jetzt die verfügbaren Werte, wenn die Eigenschaften `noApplet=true` und `sorted=true` gesetzt sind. (ID-12823).
- Für Endbenutzer werden keine Popup-Dialogfelder mehr angezeigt, wenn sie sich bei einer verschlüsselten Site anmelden bzw. aus dieser abmelden. (ID-13054).

- In Formularen, die eine Zusammenfassung zu Kontenpasswortrichtlinien geordnet nach Ressourcen anzeigen, lassen die Ressourcen diese Informationen jetzt innerhalb einer Tabelle erscheinen. In früheren Versionen liefen diese Informationen über die rechte Seite des Browser-Fensters. (ID-13109).
- In der Datei `sysconfig` steuert der Parameter `security.delegation.historyLength` jetzt die Anzahl der vorher protokollierten Delegierungen. (ID-13141).
- Die Admin-Version von `continueLogin.jsp` zeigt Katalogmeldungen jetzt richtig an. (ID-13193).
- Ein „Null-Zeiger"-Ausnahmefehler, der ausgelöst wurde, wenn ein Benutzer die Bearbeitung einer Ressource nach einer Suche bzw. Filterung abbrach, tritt jetzt nicht mehr auf. (ID-13434).
- Beim Erstellen einer neuen Rolle wird „Verfügbare Ressourcengruppen" nicht mehr zweimal auf der linken und rechten Seite des Fensters angezeigt. (ID-13573).
- Durch das Kopieren einer vorhandenen Ressource durch Umbenennen der betreffenden Ressource und anschließende Auswählen von „Erstellen" anstatt „Umbenennen" werden die Ressourcenkomponenten (z.B. ob `ActiveSync` aktiviert ist) jetzt korrekt dupliziert. (ID-14175).
- Das Freigeben und Sperren von Konten funktioniert jetzt ordnungsgemäß, wenn die Kontorichtlinie in der Service Provider-Hauptkonfiguration nicht gesetzt ist. In früheren Versionen funktionierte die Schaltfläche „Sperren" auf der Service Provider-Seite zum Bearbeiten von Konten nur dann, wenn für den betreffenden Service Provider eine Kontorichtlinie konfiguriert war. (ID-14181).

Formulare

- Die Sortierfunktion der Anzeigeklasse „SortingTable" verursacht bei manuellen Aktionen keinen Fehler mehr. (ID-12508).
- Meldungen zu Verifizierungsregeln werden jetzt im Gebietsschema des Clients und nicht dem des Servers angezeigt. (ID-12780).

Identity Auditor

- Überprüfungsrichtlinien können jetzt so konfiguriert werden, dass nur eine beschränkte Anzahl an Ressourcen abgefragt wird. (ID-9127).
- Es können jetzt auch indirekt zugewiesene Richtlinien angezeigt werden. (ID-11886).
- `UserViewConstants.OP_CALL_VIEW_VALIDATORS` kann für die Richtlinienüberprüfung während des Provisionings gesetzt werden. (ID-12757).

- Richtlinienüberprüfungen bei Vorgängen zum Benutzer-Provisioning können im Provisioning-Thread ausgeführt werden. In früheren Versionen wurde zum Ausführen einer solcher Überprüfung stets eine getrennte Aufgabe erstellt. Wenn ein Aufgabenverhalten benutzerspezifisch angepasst wurde, konnte es vorkommen, dass beim Umgehen dieser Aufgabe die benutzerspezifischen Einstellungen nicht verwendet wurden. Zum Beheben dieses Problems ist das Systemkonfigurationsattribut `user.view.alwaysUseTask` auf „true“ zu setzen. Dadurch wird das frühere Verhalten erzwungen. (ID-14086).

Identity Manager SPE

- Der Zeitgeber für Transaktionsereignisse wird während einer Transaktion nicht neu gestartet. In früheren Versionen war in der Zeit zur Transaktionsverarbeitung in Identity Manager SPE nicht die Zeitdauer zur Kontenrichtlinienevaluierung enthalten. (ID-14416).
- Identity Manager SPE setzt jetzt die Transaktionsverabeitung fort, wenn ein Dienst abnormal beendet wird, z.B. wenn der Anwendungsserver mit einem „Out-of-memory“-Fehler (nicht genügend Speicher) abbricht. (ID-14579).

Lokalisierung

- Als Authentifizierungsfragen verwendete Meldungsschlüssel werden auf der Ergebnisseite jetzt ordnungsgemäß angezeigt. (ID-13076).

Mainframe

- Der RACF-Adapter sucht für jeden einzelnen in `listAllObjects` aufgeführten Benutzer keine lange Zeichenkette mehr. Dadurch wird diese Funktion bei einer großen Benutzeranzahl schneller. (ID-12829).

Berichte

- In Überprüfungsberichten erscheinen alte Attributwerte jetzt ordnungsgemäß. (ID-12287).
- Die Generierung zu langer `TaskTemplate`-Namen (d.h. länger als MAX_NAME_LENGTH) wurde behoben. (ID-13790).

Repository

- Bei der Verwendung von Oracle 10g als Repository unter hoher Belastung (z.B. mit mehr als 100 000 Benutzern) kann die Systemgeschwindigkeit beim Erstellen und Ändern von Benutzern u.U. abfallen. Zur Wiederherstellung der ursprünglichen Systemleistung sollten Sie versuchen, die Statistik für die Tabelle `userobj` mit der folgenden SQL-Anweisung zu aktualisieren: (ID-14605).

  ```
  analyze table waveset.userattr compute statistics;
  ```

Ressourcen

- Das Ressourcenattribut `removeDenyGroupsDuringDelete` für den Domino-Ressourcenadapter gibt an, ob ein Benutzer aus einer Verweigerungsgruppe entfernt werden soll, wenn er in Identity Manager gelöscht wird. Durch Setzen dieses Attributs auf „true“ wird angegeben, ob das Entfernen aus den Gruppen bearbeitet werden soll. Aus Gründen der Abwärtskompatibilität ist der Standardwert für dieses Attribut „false“. (ID-10466).
- Der LDAP-Adapter generiert für ein neues Konto keinen unzulässigen Distinguished Name (DN) mehr. (ID-10951).

  Die escape-Methode in `com.sun.idm.util.ldap.DnUtil` kann jetzt in Formularen verwendet werden, um Werte, die in Identitätsvorlagen von Ressourcenadaptern im LDAP DN-Format eingefügt werden sollen, zu überspringen. Als Alternative kann eine `accountId`-Richtlinie mit aktivierter Option “LDAP-DN-Format verlangen” verwendet werden, um LDAP DNs, die z.B. durch Benutzer, ActiveSync oder Abstimmungsrichtlinien in Identity Manager eingegeben werden, zu validieren.
- Die Normalisierungsmethode in `RFC2253Parser` erkennt jetzt unzulässige LDAP DNs und meldet diese. (ID-10952).
- Die Methode `getNextIndex` von `DblBufferIterator` greift nicht mehr auf Kapazitätsinformationen unterstützender Arrays außerhalb der Objektsynchroniserung zu. (ID-11129).
- Der Synchronisierungsstatus in Cluster-Umgebungen wurde verbessert. (ID-11250).
- Die Methode `isPickListAttribute` von `com.waveset.adapter.SiebelResourceAdapter` wird vom Verfolgungssystem nicht mehr fälschlicherweise als `isMVGAttribute` erkannt. (ID-11471).
- Der Standardwert für das ActiveSync-Attribut **Zu synchronisierende Objektklassen** auf LDAP-Ressourcen ist jetzt standardmäßig `inetorgperson`. (ID-11644).
- Die Maximalanzahl der in einer ActiveSync-Ressource konfigurierten Flat File Active Sync-Protokolle wird jetzt ordnungsgemäß erzeugt. (ID-11848).
- Die Zuweisung des Attributs `objectClass` ist für Schema-Maps von LDAP-Ressourcen nicht mehr erforderlich, damit Active Sync funktioniert. Benutzerspezifische Ressourcenadapter, die `com.waveset.adapter.LDAPResourceAdapter` durch Überschreiben der Methoden `poll()` und `getUpdateRows(UpdateRow)` erweitern, sind so zu ändern, dass in jeder Methode `LDAPResourceAdapterBase.ensureObjectClassInSchemaMap()` aufgerufen wird. (ID-11880).

- Der Domino-Ressourcenadapter unterstützt jetzt das Setzen der Option „ID in einer Datei speichern" als Ressourcenattribut auf „false". Dadurch wird das Erstellen der Benutzer-ID-Datei auf der lokalen Festplatte verhindert. Die ID-Datei muss jedoch beim Erstellen eines Benutzers verfügbar sein. (ID-12139).
- Solaris- und Linux-Adapter liefern jetzt Anmeldeinformationen des letzten Jahres. (ID-12182).
- Der Oracle ERP-Adapter schließt jetzt Oracle-Datenbankzeiger. In früheren Versionen schloss der Adapter diese Zeiger nicht, was nach einiger Zeit die Fehlermeldung „`ORA-01000: maximum open cursors exceeded`" auslöste. (ID-12222).
- Fehler für gesperrte Konten bzw. Benutzer von Active Sync werden jetzt protokolliert. (ID-12446).

  Wenn mit Active Sync ein Fehler auftritt, weil ein Konto bzw. Benutzer, das/der aktualisiert werden soll, von einem anderen Prozess gesperrt ist, wird das betreffende Konto/der betreffende Benutzer in `syslog` protokolliert. Das ermöglicht das erneute Ausführen dieser Transaktion, wenn das Konto bzw. der Benutzer nicht mehr gesperrt sind.
- Beim Domino-Ressourcenadapter rufen gleichzeitige Aktualisierungen von `HTTPPassword` mit mehreren Benutzern mithilfe der API `NSFNoteComputeWithForm()` keinen Gateway-Fehler „-551" mehr hervor. (ID-12466).
- Gateway-Abstürze ereignen sich nicht mehr für Kunden, die APIs direkt ohne den Zugriff auf Identity Manager nutzen. (ID-12481).
- Der Flat File Active Sync-Adapter zeigt jetzt im Active Sync-Protokoll (falls aktiviert) einen Warnhinweis an, wenn ein Fehler auftritt, der für Synchronisierungszwecke eine `diff`-Aktion verhindert. (ID-12484).
- Die zum Erstellen eines Natural-Ressourcenadapters verwendete Terminalemulation wurde so geändert, dass Benutzernamen mit 8 Zeichen Länge zur Auswahl des Attributs „Copy Links" kein Tabulatorzeichen verwenden. (ID-12503).
- Änderungen des Objekts `AttrParse` erfordern keinen Neustart mehr, damit die geänderten Werte wirksam werden. (ID-12516).
- Der Siteminder LDAP-Adapter führt jetzt die folgenden Operationen auch dann ordnungsgemäß aus, wenn Siteminder-Benutzer aufgrund fehlgeschlagener Anmeldungen gesperrt wurden. (ID-12824).
  - Aktivieren
  - Deaktivieren
  - Passwort ablaufen lassen (mit Aktivierung/Deaktivierung)
  - Passwort nicht ablaufen lassen (mit Aktivierung/Deaktivierung)

- Die Änderung von LDAP-Gruppenmitgliedschaften nutzt jetzt einzelne Hinzufüge- und Entfernungsvorgänge, anstatt die gesamte Gruppe zu ändern (d.h., das gesamte Attribut `uniqueMember` wurde ersetzt). (ID-13035).
- Identity Manager setzt vor dem Löschen eines Benutzers mit sicherem ID jetzt Admin-Zugriffsrechte (falls vorhanden) zurück. (ID-13053).
- Ein Zeigerleck im Oracle-Tabellenadapter (`DatabaseTableResourceAdapter`) wurde behoben. (ID-13111).
- Die komplexe Attributsyntax von `auditorObject` für die Oracle ERP-Ressource wurde geändert und enthält jetzt einen Namensraum zum einfacheren Abrufen von Informationen aus dem `GenericObject`. Die Syntax des Attributs enthält jetzt "auditorResps" auf der obersten Stufe, die eine Liste von Responsibility-Objekten enthalten. (ID-13302).
- An `AttrParse` wurde Leistungsverbesserungen vorgenommen. Der normale Parserprozess löst nicht mehr für jedes Zeichen im Puffer einen Ausnahmefehler aus (und fängt diesen auch nicht mehr ab). (ID-13384).
- SecurID für UNIX-Adapter führt bei der Zusammenarbeit mit RSA jetzt UTF-8-Codierung und -Decodierung aus. (ID-13451).
- Beim Erstellen eines Kontos auf einer Windows NT-Ressource über den Windows NT-Ressourcenadapter wird auf der Ergebnisseite „Benutzer erstellen" die folgende Fehlermeldung nicht mehr angezeigt: „`Error requiring password: put_PasswordRequired(): 0X80004005:E_FAIL`". (ID-13618).
- Das Active Directory-Attribut `PasswordNeverExpires` kann jetzt auch während einer Aktualisierung gesetzt werden. (ID-13710).
- Identity Manager 7.0 Server benachrichtigt nach dem Abbauen einer Verbindung über das Gateway wartende Threads jetzt durch Aufruf von `notify`. (ID-14044).

Sicherheit

- Ein Benutzer mit der Fähigkeit „Organisations-Administrator" für eine Organisation kann keine Organisationen in anderen Organisationen mehr erstellen, auch wenn dieser Benutzer die Fähigkeiten „Konto-Administrator" und „Rollen-Administrator" besitzt. (ID-10235).
- Die Passwortgenerierung erfolgt jetzt auch für Passwörter, die keinen Richtlinien entsprechen, ordnungsgemäß. (ID-12275).
- In der Admin-Oberfläche wird jetzt ein Warnhinweis zum Passwortablauf angezeigt. (ID-13236).

- Benutzer mit der Fähigkeit „Genehmiger“ haben keine Zugriffsrechte mehr auf den Typ „RemediationWorkItem“. (ID-14163).

  Für Installationen vor Identity Manager 7.0 hat ein Genehmiger für den Typ `WorkItem` vollständige Rechte. Die Authentifizierungstypen `RemediationWorkItem` und AttesationWorkItem sind von `WorkItem` abgeleitet. Deswegen besitzt ein Genehmiger vollständige Zugriffsrechte auf `RemediationWorkItems` und möglicherweise andere `Attestations` (Bescheinigungen) von Benutzern.

  Dieses Problem wurde in den neuen Identity Manager 7.0-Installationen und bei Installationen, die auf Identity Manager 7.0 aufrüsten, behoben. Zur Abwärtskompatibilität kann bei Installationen vor Identity Manager 7.0 dieses Problem auf die folgende Weise behoben werden:

  a. Alle Referenzen auf die Fähigkeit „Genehmiger“ sind in die neue Fähigkeit „Genehmiger-Administrator“ zu ändern. Dazu gehören Referenzen auf die Admin-Gruppe eines Benutzers oder Workflows, die die Fähigkeit „Genehmiger“ zuweisen.

  b. Vergewissern Sie sich, dass alle in Workflows erstellten Arbeitseinheiten den angegebenen `authType` besitzen. Falls das nicht der Fall ist, ist der `authType` = Approval.

  c. Führen Sie `WorkItemUpdater` in `update.xml` aus, um alle Arbeitseinheiten ohne `authType` auf den `authType` Approval zu setzen (mit dieser Funktionen kann jeder beliebige `authType` eingestellt werden). Die Anweisungen befinden sich in der Datei, sind jedoch standardmäßig auskommentiert.

- Für Benutzer ohne Administrator-Fähigkeiten sind jetzt Rollen und Ressourcen sichtbar. (ID-14745).

  Früher waren Rollen und Ressourcen nicht für Benutzer verfügbar, die keine Admin-Rechte für Organisationen besaßen. Wenn ein solcher Benutzer “Eigene Rollen aktualisieren” oder “Eigene Ressourcen aktualisieren” auswählte, waren weder Rollen noch Ressourcen zur Auswahl sichtbar.

Server

- Von `TaskInstance` abgeleitete Objekte wie z.B. Genehmigungen werden jetzt bei Beendigung einer Aufgabe ordnungsgemäß gelöscht. (ID-3258).
- In Formularen funktioniert die Methode `<set>` innerhalb von `<Expansion>` jetzt ordnungsgemäß. (ID-9617).
- Der letzte Überprüfungseintrag geht nicht mehr verloren, wenn eine Aktion aufgrund des Umbenennens einer Ressource fehlschlägt. (ID-9714).

- In Cluster-Umgebungen erzeugt eine fehlgeschlagene Anmeldung auf den Endbenutzerseiten keinen Serialisierungsausnahmefehler mehr. (ID-10556).
- Ein Server versucht sich nicht mehr als aufgehängt zu identifizieren, wenn die Aufgabenbearbeitung lange dauert. (ID-10920).
- Das IAPI-Objekt „Configuration" wurde in das IAPI-Objekt „XmlData" migriert, das vorrangig von ActiveSync-Ressourcen zum Speichern von Informationen zur letzten bearbeiteten Änderung genutzt wird. (ID-11266).

  Das Laden von `update.xml` verursacht, dass das ResourceUpdater-Objekt vorhandene „High water mark"-Daten vom IAPI-Objekt „Configuration" in ein XmlData-Objekt mit dem angezeigten Namen „SYNC_resourceName" migriert und das ursprüngliche Configuration-Objekt entfernt.
- Referenzen auf Server und Viewer vom Typ „Session", die in Identity Manager 5.0 SP1 verworfen wurden, sind entfernt worden. (ID-11873).
- Die Verarbeitung von Begrenzungszeichen wird jetzt zwischen eckigen Klammern unterdrückt. Als Folge davon werden jetzt alle zwischen eckigen Klammern erkannten Zeichen als Index oder Filter interpretiert. Hinweis: Gegenwärtig existiert kein Verfahren zum Umschalten nach Erkennung der schließenden eckigen Klammer „]". (ID-12384).
- Der `changelog`-Dateiname darf jetzt im Präfix Punkte (.) enthalten. (ID-12470).
- Das Beenden von Aufgabeninstanzen wird jetzt als Terminate-Aktion anstatt Modify-Aktion protokolliert. (ID-12791).
- Die Erstellung von Account-Objekten wurde beschleunigt, was auch eine Leistungsverbesserung bei Abstimmungen und Provisionings zur Folge hat. (ID-13341).
- Eine neue Einstellung zur Serverkonfiguration unter Konfigurieren->Server ermöglicht das Einstellen einer Maximalanzahl an Aufgaben, die auf einem Server gleichzeitig ausgeführt werden können. (ID-13343).

Workflow

- Verschachtelte Referenzen auf den Namen einer Regel, die sich in der gleichen Bibliothek befindet, der aber der Bibliotheksname nicht vorangestellt ist, können jetzt aufgelöst werden, und der Fehler „Ungelöste Regel" tritt nicht mehr auf. (ID-10265).
- Wenn Meldungen mithilfe von `notification.rediret` in eine Datei umgeleitet werden, wird diese Datei jetzt mithilfe der Methode `emailNotifier.contentCharset` geschrieben. Diese Methode dient auch zum Erstellen von E-Mails aus Meldungen. Dadurch kann die Datei auch Zeichen enthalten, die nicht im ISO-8859-1-Zeichensatz enthalten sind. (ID-10331).

- Workflow-Meldungen enthalten ausführlichere Informationen, wenn ein Genehmiger Arbeitseinheiten genehmigt oder ablehnt, die bereits genehmigt bzw. abgelehnt wurden. (ID-11045).
- Der Debugger ist jetzt standardmäßig aktiviert. Für den Einsatz unter Produktionsbedingungen wird die Deaktivierung des Debuggers durch Einstellen der Systemkonfigurationeigenschaft „`serverSettings.default.debugger.enabled=false`“ empfohlen. (ID-14076).

Dokumentation

Im Zuge der Integration von Identity Auditor und der Service Provider Edition in Identity Manager für diese Version wurden die folgenden Dokumentationen verworfen:

- *Identity Auditor Administration*
- *Identity Manager Service Provider Edition Administration Addendum*
- *Identity Manager Audit Logging*

Der Inhalt dieser Dokumente befindet sich jetzt im *Identity Manager Administration* Guide.

Weitere behobene Probleme

10475, 11052, 12452, 13434, 14178

Bekannte Probleme

Die folgenden Abschnitte enthalten bekannte Probleme und Zwischenlösungen für:

- Identity Manager
- Service Provider Edition
- Auditor

Identity Manager

Allgemein

- Falls versucht wird, auf bestimmte Seiten zuzugreifen, wenn Cookies deaktiviert sind, wird eine Eingabeaufforderung für die Anmeldung aufgerufen (ID-158).
- Systeme, die Sun Identity Manager Gateway ausführen, müssen so konfiguriert werden, dass Dr. Watson keine visuellen Benachrichtigungen erzeugt. Wenn diese Funktion festgelegt ist und beim Gateway ein Fehler auftritt, kann der Prozess erst ausgeführt werden, nachdem das Popupfenster geschlossen wurde.
- Die Variablen display.session und display.subject sind für Disable-Formularelemente nicht verfügbar. Erstellen Sie nach Möglichkeit keine potenziell langen Aktivitäten in Disable-Elementen, weil diese Ausdrücke immer ausgeführt werden, wenn das Formular neu berechnet wird. Führen Sie stattdessen die Berechnung in einem anderen Formularelement aus, das nicht so oft ausgeführt wird.
- Mit dem OpenSPML-Toolkit von Identity Manager erzielen Sie bei der Arbeit mit der Identity Manager-Weboberfläche optimale Ergebnisse. Bei Verwendung der Datei `openspml.jar` von der Website openspml.org aus können Speicherfehler auftreten. (ID-11889).

- Wenn im Identity Manager-Installationsverzeichnis freier Platz verfügbar ist, müssen Sie die Umgebungsvariable WSHOME ohne doppelte Anführungszeichen (") wie unten gezeigt angeben.

HINWEIS Nachstehende umgekehrte Schrägstriche (\ ) dürfen bei der Pfadangabe auch dann nicht verwendet werden, wenn der Pfad keine Leerzeichen enthält.

```
set WSHOME=c:\Program Files\Apache Group\Tomcat 4.1\lighthouse
```

oder

```
set WSHOME=c:\Progra~1\Apache~1\Tomcat~1\lighthouse
```

Folgende Angaben sind ungültig:

```
set WSHOME="c:\Program Files\Apache Group\Tomcat 4.1\lighthouse"
```

- Erforderliche Felder, die in der Ressourcenschemazuordnung festgelegt wurden, werden nur beim Erstellen von Benutzerkonten geprüft (ID-220). Wenn ein Feld bei Benutzeraktualisierungen benötigt wird, ist das Benutzerformular entsprechend zu konfigurieren.
- Organisationsname, Administratorname, Kontoname, Name des Benutzerattributs (links in der Schemazuordnung) und Aufgabennamen werden nicht auf ungültige Zeichen geprüft (ID-1145, 1206, 1679, 1734, 1767, 2413, 3331). In den Namen für diese Objekttypen sind folgende Zeichen nicht zulässig: Dollar ($), Komma (,), Punkt (.), Apostroph ('), kaufmännisches Und (&), linke eckige Klammer ([ ), rechte eckige Klammer ( ]) und Doppelpunkt (:).
- Wenn Sie versuchen, eine Aktion nach einem Sitzungstimeout auszuführen, wird auf der Kontoseite eine irreführende Fehlermeldung angezeigt (ID-1223).
- Das Kalenderobjekt wird nicht vollständig angezeigt, wenn der Browser große Schriftarten verwendet (ID-2120).
- Das Kontrollkästchen „Alle auswählen“ auf der Suchergebnisseite und der Aufgabenliste wird nicht deaktiviert, wenn eines der Listenelemente deaktiviert ist (ID-5090). Das Kontrollkästchen „Alle auswählen“ wird während einer sich ergebenden Aktion ignoriert, wenn nicht die Kontrollkästchen aller Listenelemente aktiviert sind.
- Damit die Änderungen in einem benutzerspezifischen Meldungskatalog auch übernommen werden, ist der Server neu zu starten. (ID-6792).

- Die Registerkarten der Randleiste (beispielsweise „Kontenliste“, „Benutzer suchen“) werden auf der Bestätigungsseite nicht angezeigt, wenn mehrere Benutzer aktiviert oder deaktiviert werden (ID-6866). Nach Bestätigung der Seite werden die Registerkarten wieder eingeblendet, sobald die Ergebnisse angezeigt werden.
- Das derzeitige Verfahren zum Ermitteln eines fehlgeschlagenen Servers geht davon aus, dass alle Systeme eines Identity Manager-Clusters zeitsynchronisiert sind (ID-7064). Wenn bei dem Standardausfallintervall von fünf Minuten ein Server fünf Minuten lang nicht mit einem anderen Server synchron läuft, deklariert der Server, der zeitlich voraus ist, den zeitlich nachstehenden Server für inaktiv, was unvorhersehbare Ergebnisse zur Folge haben kann. Als Zwischenlösung muss eine bessere Zeitsynchronisierung eingerichtet oder das Failover-Intervall erhöht werden.
- Wenn Sie sich unter Windows mit einem Benutzernamen mit Doppelbytezeichen anmelden und die Standardzeichnsätze für den Computer nur Einzelbytezeichen unterstützen, müssen Sie die Umgebungsvariable USER_JPI_PROFILE auf ein vorhandenes Verzeichnis setzen, dessen Name nur Einzelbytezeichen enthält. (ID-8540).

Installation und Aktualisierung

- Bei der Identity Manager-Installation über die Datei `idm.war` sind die Ausführungskomponenten in den UNIX-Shellskripten nicht festgelegt (ID-2371). Zwischenlösung: Führen Sie den UNIX-Befehl „chmod“ im Verzeichnis `idm/bin` aus.
- Wenn Identity Manager in einer Tomcat 5.x-Umgebung installiert ist, wird bei der Ausführung von Berichten ein Java-Fehler erzeugt (ID-6652). Es gibt folgende Zwischenlösung:

  ```
  cd $WSHOME\WEB-INF\classes

  jar xvf ..\lib\j2ee.jar javax/activation/DataSource.class
  ```
- Die AD ActiveSync-Ressource wurde verworfen und durch die AD-Ressource ersetzt. Führen Sie folgende Schritte aus, um zu AD ActiveSync für neuere Versionen zu migrieren: (ID-11363).
  - Exportieren Sie das vorhandene AD ActiveSync-Ressourcenobjekt in eine XML-Datei (über die Befehlszeile oder auf den Debug-Seiten).
  - Löschen Sie die vorhandene Ressource (von diesem Vorgang sind keine Benutzer von Identity Manager oder des Ressourcenkontos betroffen).

  - Erstellen Sie eine neue AD-Ressource als ActiveSync-Ressource.
  - Exportieren Sie dieses neue Ressourcenobjekt in eine XML-Datei.
  - Setzen Sie in dieser Datei die Werte für dieAttribute „id“ und „name“ auf die Werte des ALTEN, in Schritt 1 gespeicherten Ressourcenobjekts. Diese Attribute befinden sich im Tag `<Resource id='`*`ID-Nummer`*`' name='AD' ...>`.
  - Speichern Sie die Änderungen in der Datei.
  - Importieren Sie das geänderte Objekt zurück in Identity Manager. Verwenden Sie hierzu die Seite „Konfigurieren->Exchange-Datei importieren“ oder die Befehlszeile.

- Wenn Sie eine 6.x-Installation aktualisieren, aber die neuen Endbenutzerseiten verwenden möchten, müssen Sie den Systemkonfigurationsparameter `ui.web.user.showMenu` manuell auf „true“ setzen, damit die horizontale Navigationsleiste angezeigt wird. (ID-14900).

Kontoverwaltung

- Es können jetzt NT-Konten erstellt werden, die mehr als 20 Zeichen lang sind und von den nativen NT-Tools nicht unterstützt werden (ID-710).
- Ein Administrator kann nur Ressourcen oder Rollen speichern, deren Organisationen von ihm verwaltet werden (ID-839).
- Beim Sortieren der Spalten auf der Seite für die Bereitstellungsergebnisse werden zu den Ergebnissen zusätzliche leere Zeilen hinzugefügt (ID-1105).
- Genehmigungen für mehrere hundert Benutzerkonten dauern sehr lange (ID-1149). Zwischenlösung: Organisieren Sie die Datensätze für die Benutzerkonten in kleineren Gruppen.
- Die Genehmigungsdatensätze eines Administrators, der nicht mehr über eine Genehmigungsberechtigung verfügt, können nicht genehmigt werden (ID-1150). Zwischenlösung: Entfernen Sie den Administrator aus den Ressourcen, Rollen und Organisationen, für die Genehmigungsrechte bestehen, und genehmigen Sie anschließend alle ausstehenden Genehmigungsdatensätze, bevor Sie den Administrator oder die Genehmigungsberechtigung für den Administrator entfernen.
- Wenn ein Benutzer ohne Änderungen aktualisiert wird, wird die detaillierte Ergebnisseite nicht angezeigt (ID-2327).

- Wenn Sie einen neuen Benutzer erstellen oder eine Ressource zu einem vorhandenen Benutzer hinzufügen und der DN für den Benutzer falsch ist, wird der falsche Wert solange zwischengespeichert, bis sich der Administrator abmeldet (ID-2508). Wenn der DN korrigiert wurde, kann der Benutzer erst neu erstellt werden, nachdem sich der Administrator abgemeldet hat.
- Die Kontosperrmeldung wird im Anmeldefenster der Identity Manager-Benutzeroberfläche von Netscape 4.7 nicht angezeigt (ID-2680). Die Fehlermeldung wird im Seiten-URL angezeigt.
- Die Bezeichnung „name" ist ein für die Ansicht reserviertes Wort und kann nicht als Identity Manager-Benutzerattribut für Ressourcenschemazuordnungen verwendet werden (ID-2918).
- In Windows Active Directory muss das Gateway als Administrator, der Verzeichnisse erstellen kann, ausgeführt werden (ID-2919). Identity Manager kann Ausgangsverzeichnisse unter Windows 2000 erstellen. Der Kontoerstellvorgang für ein Ausgangsverzeichnis wird nicht vom in der Ressourcendefinition angegebenen Administrator, sondern vom Benutzer, unter dem der Gatewayprozess läuft, ausgeführt. Zwischenlösung: Geben Sie statt des Benutzers, unter dem das Gateway auf dem lokalen System läuft, ein Konto an, das über Berechtigungen zum Erstellen von entfernten Freigaben verfügt, und legen Sie die Berechtigungen für diese Freigaben fest. Dieses Konto muss außerdem die durchsuchende Überprüfung umgehen und als Betriebssystemberechtigung fungieren.
- Die Windows NT-Ressource erzeugt eine Warnmeldung anstelle einer Fehlermeldung, wenn beim Deaktivieren eines Benutzerkontos ein Fehler auftritt (ID-3222).
- Es wird manchmal eine java.lang.NullPointerException angezeigt, wenn auf der Seite zum Bearbeiten von Benutzern alle Ressourcen aus einem Benutzer entfernt werden (ID-4811). Zwischenlösung: Trennen oder löschen Sie diese Ressourcenkonten auf der Seite zum Löschen von Benutzern aus dem Benutzer.
- Wenn ein Identity Manager-Benutzer erstellt und einer Windows Active Directory-Ressource zugewiesen wird, in der das Benutzerkonto bereits vorhanden ist, wird der Benutzer ohne GUID-Attribut in den Ressourceninformationen erstellt (ID-5114). Diese GUID ermittelt Änderungen bei der Organisation oder dem Namen des Benutzers in Active Directory. Sie können dieses Problem beheben, indem Sie in der Ressource eine Abstimmung ausführen.

- Beim Erstellen eines Benutzers wird eine Warnung ausgegeben, falls Sie dem Benutzer eine Rolle hinzufügen, die eine direkt zugewiesene Ressource enthält (ID-5385).
- Ein „Weiterleiten an“-Administrator kann nicht angegeben werden, wenn ein Benutzer erstellt wird. Diese Option kann nur festgelegt werden, wenn der Benutzer bearbeitet wird (ID-5695).

Genehmigungen

- Wenn Sie einen Benutzer im Hintergrund aktualisieren, wird auf der Seite für die Aufgabenergebnisse eine Genehmigungsaktivität angezeigt (ID-3301). Diese Genehmigung kann ignoriert werden.
- Die Genehmigungsdatensätze für einen Administrator werden erst angezeigt, nachdem der Benutzer umbenannt wurde (ID-3386). Zwischenlösung: Bearbeiten Sie alle ausstehenden Genehmigungen, bevor Sie den Benutzer umbenennen.
- Zuvor genehmigte oder abgelehnte Genehmigungsdatensätze können von einem Administrator nicht angezeigt werden, wenn der zu genehmigende Benutzer einer Organisation angehört, die der Genehmiger nicht steuert (ID-3494).
- Ressourcenwiederholungsaufgaben werden in der ausstehenden Genehmigungsliste für den Configurator angezeigt (ID-3508).

Integrierte Entwicklungsumgebung (IDE)

- Für die meisten Knoten existiert im Fenster „Eigenschaften“ ein zugehöriges Eigenschaftsarbeitsblatt, und sie besitzen die Eigenschaft „name“ zum Speichern einer Knotenbezeichnung. Wenn Sie ein Objekt über seinen Knoten (durch Klicken auf das Objekt mit der rechten Maustaste und Auswahl von „Umbennen“) umbenennen, wird die Knotenbezeichnung aktualisiert und die XML-Daten ändern sich entsprechend. Die Änderung wird jedoch im Arbeitsblatt nicht übernommen. Wenn Sie auf einen anderen Knoten und danach erneut auf den umbenannten Knoten klicken, erscheint der neue Name im Eigenschaftsarbeitsblatt. Sie können auch auf den Titel des Arbeitsblatts klicken, damit der richtige Wert übernommen wird. (ID-13696).
- Objekte, die die Identity Manager IDE verwenden, sollten über das durch Rechtsklick aufrufbare Kontetxmenü im Projekt-Explorer und nicht durch direktes Bearbeiten von XML-Daten im Editor umbenannt werden. (ID-13828).

- Der XML-Navigator wurde in der IDM IDE deaktiviert. Das Navigator-Fenster wird über „Fenster ->Navigator“ geöffnet, und es wird <No view available> angezeigt. (ID-13390).
- Das Löschen von Projekten wird nicht unterstützt. (ID-14013).
- Regelbibliothekn werden zurzeit nur für grundlegendes Bearbeiten und Testen von XML-Code im Regeltester unterstützt. Navigations- und Eigenschaftsunterstützung ist zurzeit nicht implementiert. (ID-14093).
- Formulareigenschaftswerte können nicht mit dem Eigenschafts-Editor bearbeitet werden, wenn der Datentyp Integer oder Boolean ist. (ID-14128).

  Zwischenlösung: Der betreffende Eigenschaftswert ist direkt im XML-Code zu setzen.
- Das Herunter, Hoch- oder Neuladen eines Objekts verursacht eine Sperrung des betreffenden Objekts im Repository. Infolgedessen können Zugriffe auf dieses Objekt durch Benutzer, die nicht in den Projekteinstellungen angegeben sind, innerhalb der vorgesehenen Sperrzeit fehlschlagen. (ID-14132).
- Zum Vermeiden von Anzeigeproblemen mit der Entwurfsleiste und der Workflow-Symbolleiste sollte die erweiterte Option „Show ToolBar“ stets aktiviert sein. (ID-14138).
- Beim Schließen eines Projekts funktioniert die Option „Discard All“ nicht ordnungsgemäß. Wenn Sie alle an einem Objekt vorgenommenen Änderungen verwerfen wollen, müssen Sie das Editorfenster schließen und „Discard“ auswählen. Dies ist ein bekanntes NetBeans-Problem (Bug-ID 84326). (ID-14164).
- Damit ein Objekt über das Kontextmenü in NetBeans umbenannt werden kann, muss diese Änderung gespeichert werden. Nach dem Vornehmen der Änderung können Sie diese über „Datei ->Speichern“ speichern, ohne die Datei öffnen zu müssen. Wenn die Datei geöffnet ist, können Sie „Datei ->Speichern“ verwenden oder die Datei schließen und die Änderungen speichern, wenn Sie dazu aufgefordert werden (ID-14420).
- Wenn Sie „displayClass“ eines Feldes auf „InlineAlert“ setzen, wird der InlineAlert-Wert nicht angezeigt, wenn das Feld in der Werteigenschaft einen Namen enthält. (ID-14456).
- Das Auschecken einer Benutzeransicht in Identity Manager IDE sperrt das betreffende Objekt. Durch das Einchecken bzw. Schließen der Ansicht wird die Sperre nicht sofort, sondern automatisch nach 5 Minuten aufgehoben. Sie können die Sperre auch aufheben, indem Sie sich in Identity Manager als der Administrator anmelden, der die Ansicht in der IDM IDE ausgecheckt hatte und den Benutzer anzeigen. (ID-14797).

Anmeldekonfiguration

- Das Modul für die Pass-Through-Authentifizierung funktioniert bei der Domino-Ressource nicht (ID-1646).
- Änderungen bei den Seiten für das Setup für die Administrator- und Benutzeranmeldung werden anderen angemeldeten Administratoren nicht angezeigt (ID-3487). Um die Änderungen anzuzeigen, müssen sich die anderen Administratoren bei der Administratorbenutzeroberfläche abmelden und anschließend wieder anmelden.
- Wenn sich ein Administrator anmeldet, „Mein Passwort ändern" auswählt und anschließend eine andere Registerkarte anklickt, wird das Konto gesperrt, bis die Sperre abgelaufen ist. (ID-3705).

  Wenn ein anderer Administrator versucht, den gesperrten Administrator zu bearbeiten, wird folgende Meldung angezeigt: „com.waveset.util.WavesetException: Auf Konto #ID#Configurator kann zur Zeit nicht zugegriffen werden. Versuchen Sie es später erneut." Wenn der Administrator auf „OK" klickt, wird das Workflow-Prozessdiagramm der letzten Aktion angezeigt.

Organisationen

- Wenn beim Löschen von mehreren Organisationen der Löschvorgang für eine Organisation fehlschlägt, werden die verbleibenden Organisationen auch nicht gelöscht (ID-517).
- Wenn bei einer Organisation, die zugewiesene Benutzer und ausstehende Bereitstellungsanforderungen aufweist, umbenannt wird, schlägt die Bereitstellungsanforderung fehl (ID-564). Zwischenlösung: Stellen Sie sicher, dass keine ausstehenden Anforderungen vorhanden sind, bevor Sie eine Organisation umbenennen.
- Wenn beim Erstellen einer neuen Organisation die Option für die Benutzermitgliedsregel vor der Angabe eines Organisationsnamens ausgewählt und anschließend die Seite aktualisiert wird, erscheint eine Organisations-ID im Feld für den Organisationsnamen (ID-6302). Der Name kann weiterhin vor dem Speichern der neuen Organisation festgelegt werden.

  ```
  ( ) - Achtung: In Klammer stehende Werte im Feld „Genehmiger"
  entsprechen keinem der zulässigen Werte.
  ```

Richtlinien und Fähigkeiten

- Das Identity Manager-Kontorichtlinienattribut „Rücksetzungs-Benachrichtigungsoption“ hat die Wertoption „administrator“, die keine Auswirkung hat (ID-944). Die einzig gültigen Optionen sind „sofort“ und „Benutzer“.
- Wenn beim Löschen von mehreren Rollen ein Fehler auftritt, wird nicht mit den anderen Rollen fortgefahren, sondern der gesamte Vorgang angehalten (ID-1168).
- Die Mindestanzahl der Fragen, die ein Benutzer beantworten muss, kann auf einen Wert gesetzt werden, der größer als die Anzahl der definierten Fragen ist (ID-1834). In diesem Fall kann sich der Benutzer nicht über die Option „Passwort vergessen“ anmelden.
- Die Lighthouse-Standardkontorichtlinie kann nicht durch Bearbeiten der Richtlinie, Ändern des Namens oder Erstellen eines neuen Objekts geklont werden (ID-5147). Zwischenlösung: Erstellen Sie eine neue Kontorichtlinie.

Abstimmen und Importieren von Benutzern

- Das Importieren von Benutzern aus einer CSV-Datei aktualisiert nicht die Ressourcenattribute, wenn der Benutzer bereits in Identity Manager vorhanden ist (ID-2041).
- Wenn bei einer CSV-Datei (bei der die Felder durch Kommas getrennt werden) die Konto-IDs in einfache Anführungszeichen (') gesetzt sind, werden die Anführungszeichen als Fragezeichen (?) geladen (ID-2100).
- Geplante Aufgaben werden auf der Seite „Aufgaben suchen“ nicht als Ergebnis angezeigt, wenn die Option „ist geplant“ verwendet wird (ID-5001).
- Die Abstimmung schlägt fehl, wenn sie bei einer Ressource von Red Hat Version 8 ausgeführt wird (ID-6087).
- Die Abstimmung einer Oracle ERP-Ressource wird mit Fehlern abgeschlossen, wenn bei der Ressource das Verbindungspooling aktiviert ist (ID-6386). Zwischenlösung: Deaktivieren Sie das Verbindungspooling während der Abstimmung.

Berichte

- Sicherheitsadministratoren können keine Berichte ausführen oder erstellen (ID-1217). Zwischenlösung: Erteilen Sie den Administratoren die Berechtigungen zum Berichtsadministrator.
- Risikoanalyseberichte können auch von Administratoren angezeigt werden, die keine Berichtsadministratoren sind (ID-1224).
- Berichtsergebnisse, die mit der Option für das Nur-Text-Format per E-Mail gesendet werden, sind nicht formatiert (ID-2191). Zwischenlösung: Verwenden Sie die HTML-Option für die E-Mail.
- Überwachungsprotokolleinträge werden möglicherweise bei umfangreichen Ergebnissen nicht erfasst (ID-5050).
- Die aktivierte Laufschrift wird nicht angezeigt, wenn in den Namen von Organisationen Apostrophe (') vorkommen (ID-5653).
- Wenn Sie versuchen, einen Administratorbericht auszuführen, und festlegen, dass nur Administratoren gemeldet werden, die einer bestimmten Organisation angehören, die keine Administratoren hat, wird ein java.lang.NullPointerException-Fehler zurückgegeben (ID-5722).

Ressourcen

- Über die Schaltfläche für den Ressourcentest werden nicht alle Felder getestet (ID-51).
- Zuweisungen für den Ressourcenport können auf Werte über 65535 gesetzt werden (ID-59).
- Wenn Sie einen falschen Active Directory-Gruppennamen festlegen, wird eine ungültige Fehlermeldung angezeigt (ID-393). Wenn Sie versuchen, einen Active Directory-Gruppennamen auf „groupname" statt auf „cn=groupname,cn=builtin,dc=waveset,dc=com" zu setzen, wird eine Fehlermeldung angezeigt, die besagt, dass sich der Arrayindex außerhalb der Grenzen befindet.
- Erforderliche Kontoattribute werden manchmal ignoriert, wenn eine andere Ressource mit demselben Kontoattributnamen vorhanden ist, bei der das erforderliche Flag nicht gesetzt ist (ID-1161).

- Wenn ein Administrator versucht, eine Organisation zu einer Ressource hinzuzufügen, ohne mit den zugehörigen Rechten ausgestattet zu sein, wird ein Fehler erzeugt. Die Bearbeitung der Ressource muss dann abgebrochen und anschließend wieder aufgenommen werden, um weitere Änderungen bei der Ressource vorzunehmen (ID-1274).
- Die Fehlermeldung, die bei einem falschen Ressourcenkontokennwort oder Benutzernamen erzeugt wird, ist bei einer nicht klaren PeopleSoft-Ressource falsch (ID-2235). Die Fehlermeldung lautet:

  ```
  bea.jolt.ApplicationException: TPESVCFAIL - application level service
  failure
  ```
- Bei Windows Active Directory-Ressourcenaktionen, die den Beendenstatus %DISPLAY_INFO_CODE% verwenden, schlägt die Aktion mit Fehlern fehl (ID-2827).
- Bei Windows NT-Ressourcenaktionen, die einen Beendencode ungleich null zurückgeben, schlägt die Aktion fehl (ID-2828).
- Beim Erstellen eines Benutzers kann die primäre Gruppen-ID des Benutzers in Active Directory nicht festgelegt werden (ID-3221). Zwischenlösung: Erstellen Sie den Benutzer, ohne die primäre Gruppen-ID festzulegen. Bearbeiten Sie anschließend den Benutzer und legen Sie den Wert fest. Die primäre Gruppen-ID wird außerdem nach Nummer und nicht nach DN der Gruppe festgelegt.
- Ressourcen-IP-Adressen werden in der JVM zwischengespeichert, nachdem der Hostname in eine IP-Adresse aufgelöst wurde. Wenn eine Ressourcen-IP-Adresse geändert wurde, ist ein Neustart des Anwendungsservers erforderlich, damit Identity Manager die Änderung erkennt (ID-3635). Dies ist eine Einstellung in Sun JDK (ab Version 1.3), die über die in der Regel in jre/lib/security/java.security festgelegte Eigenschaft „sun.net.inetaddr.ttl“ gesteuert wird.
- Sie können bei Oracle-Ressourcen für einen einzelnen Benutzer nicht mehrere Konten erstellen (ID-3832).
- Endbenutzer können die Selbsterkennungsfunktion nicht für Domino-Ressourcenkonten verwenden (ID-4775).

- Wenn ein Benutzer aus einem oder in einen Untercontainer innerhalb der Active Directory-Organisation verschoben wird, erkennt der ActiveSync-Adapter diese Änderung. Wenn Sie jedoch den Benutzer auf der Bearbeitungsseite anzeigen (oder eine Änderung vornehmen und die Bestätigungsseite aufrufen) wird die Konto-ID des Benutzers weiterhin als ursprünglicher DN (Distinguished Name, eindeutiger Name) angezeigt (ID-4950). Da der Benutzer über die GUID geändert wird, entstehen keine Probleme beim Betrieb. Sie können dieses Problem beheben, indem Sie für die Ressource eine Abstimmung ausführen.
- Wenn ein Benutzer aus einer Organisation (OU) in eine Unterorganisation verschoben wird, erkennt der LDAP ChangeLog-Adapter die Änderung nicht und geht davon aus, dass der Benutzer gelöscht wurde. Das Benutzerobjekt wird anschließend in Identity Manager gesperrt (wenn dies der aktuellen Einstellung entspricht), und für das verschobene Konto wird kein „neues" Konto erstellt (ID-4953).
- Die im Pool abgelegten Verbindungen für die UNIX-Ressourcenadapter können in einem nicht festgelegten Status belassen werden, wenn bei der Ausführung von Befehlen oder Skripten Fehler auftreten (ID-5406).
- NDS-Organisationen können nur dann auf der obersten Ebene der Struktur erstellt werden, wenn Sie den Basiskontext für die Ressource auf „[ROOT]" setzen (ID-5509).
- Wenn Sie in NDS ein Feld (beispielsweise die Verlängerungsfrist für die Anmeldung) während der ersten Bereitstellung bearbeiten und keine Werte für die booleschen Felder angeben, werden alle booleschen Felder auf FALSE gesetzt (ID-6770). Dadurch wird verhindert, dass die anderen Felder der Registerkarte für die Einschränkung bearbeitet werden können, weil bei denen für bestimmte Kontrollkästchenwerte TRUE gelten muss. Um dies zu vermeiden, müssen Sie stets sicherstellen, dass alle gewünschten booleschen Felder auf TRUE gesetzt sind, damit sie beim Bearbeiten anderer Felder korrekt aktiviert werden.
- Wenn Sie das Passwort für einen UNIX-Computer über die Funktion „Verbindung verwalten --> Ressourcenpasswortänderungs-Administrator" ändern, wird der Aufgabenname folgendermaßen angezeigt:

  ```
  _FM_PASSWORD_CHANGING_TASK null:null
  ```

  Es soll ein benutzerfreundlicher Name angezeigt werden. (ID-6947).
- Sie können die Funktion zum Verwalten von Verbindungen nicht für UNIX-Ressourcen einsetzen, die NIS verwenden (ID-6948). Es wird ein Fehler erzeugt, weil das Passwort, das Sie ändern möchten, für das Root-Konto bestimmt ist, das von NIS nicht verwaltet wird.

- Wenn Sie Benutzer durch Auswahl einer Aktualisierung aus einer Identity Manager-Organisation aktualisieren, erhalten Benutzer mit einem Sun One ID Server-Konto einen Fehler, falls diese nativ erstellt und in Identity Manager geladen wurden (ID-7094). Zwischenlösung: Aktualisieren Sie diese Benutzer individuell.
- Identity Manager enthält weiterhin folgende verworfenen Klassen:
  - com.waveset.object.IAPI
  - com.waveset.object.IAPIProcess
  - com.waveset.object.IAPIUser

  Angepasste Adapterklassen sollten nicht mehr auf diese Klassen, sondern auf die entsprechenden Klassen in package com.waveset.adapter.iapi verweisen (ID-8246).
- Beim Löschen eines Benutzers, der ein Konto bei der Ressource für die PeopleSoft Komponentenschnittstelle hat, tritt ein Fehler auf. Diese Ressource unterstützt derzeit nicht das Löschen von Konten. (ID-9000).

Ressourcenobjektverwaltung

- Ein Windows Active Directory-Objekt (Gruppe, Organisationseinheit oder Container) kann auf der Seite „Ressourcen auflisten“ nicht umbenannt werden (ID-3329).
- Es können keine neuen LDAP-Gruppen erstellt werden, wenn Benutzer mit CNs mit mehreren Werten vorhanden sind (ID-3848). Zwischenlösung: Verwalten Sie die Mitglieder der Gruppe nicht nach dem im LDAP-Formular zum Erstellen von Gruppen konfiguriertem CN, sondern nach dem DN.

Ressourcengruppen

- Durch Drücken der Eingabetaste auf der Seite zum Erstellen oder Bearbeiten von Ressourcengruppen werden die auf der Seite vorgenommenen Änderungen gelöscht (ID-3430).
- Berichte über Ressourcengruppen können nicht als CSV-Datei gespeichert werden. (ID-8001).

Sicherheit

- Wenn Sie ein Objekt mit Daten importieren, die mit einem Schlüssel verschlüsselt wurden, der sich nicht im Repository befindet, in das die Daten importiert werden, wird das Objekt dennoch importiert. Sie erhalten jedoch eine Warnmeldung, die besagt, dass die Daten nicht entschlüsselt werden können, weil der Serververschlüsselungsschlüssel nicht vorhanden ist. (ID-12143).

Server

Ansichten können über das Interface RemoteSession nicht zum sofortigen Einsatz erstellt werden. Der Deployment Descriptor (`web.xml`) muss aktualisiert werden. (ID-14756).

1. Fügen Sie zum Deployment Descriptor die folgende Servlet-Definition hinzu:

```
<servlet>
   <servlet-name>rpcrouter3</servlet-name>
   <display-name>OpenSPML SOAP Router</display-name>
   <description>no description</description>
   <servlet-class>
      org.openspml.server.SOAPRouter
   </servlet-class>

   <init-param>
      <param-name>handlers</param-name>
      <param-value>com.waveset.rpc.PasswordSyncHandler</param-value>
   </init-param>

   <init-param>
      <param-name>spmlHandler</param-name>
      <param-value>com.waveset.rpc.SpmlHandler</param-value>
   </init-param>

   <init-param>
      <param-name>rpcHandler</param-name>
      <param-value>com.waveset.rpc.RemoteSessionHandler</param-value>
   </init-param>
</servlet>
```

2. Fügen Sie zum Deployment Descriptor die folgende Servlet-Zuweisung hinzu:

```
<servlet-mapping>
   <servlet-name>rpcrouter3</servlet-name>
   <url-pattern>/servlet/rpcrouter3</url-pattern>
</servlet-mapping>
```

Zur Nutzung von „createView" mit „RemoteSession" muss das Servlet „rpcrouter3" verwendet werden. Damit Sie Zugriff auf das Servlet „rpcrouter3" haben, müssen Sie den Konstruktir `RemoteSession(URL, String, EncryptedData)` verwenden.

Sun Identity Manager Gateway

- Sun Identity Manager Gateway wird nicht angehalten, wenn im Fenster für die NT-Dienste die Schaltfläche zum Stoppen aktiviert wird (ID-590). Zwischenlösung: Brechen Sie die Ausführung des Stoppbefehls ab (wenn dieser immer noch inaktiv ist), und stoppen Sie den Dienst erneut; oder beenden Sie das Dialogfeld für die NT-Dienste, und führen Sie den Stoppvorgang erneut aus.
- Benutzer können in einer NT-Domäne nicht zu Gruppen hinzugefügt werden, wenn sich das Gateway in einer entfernten vertrauenswürdigen Domain befindet (ID-711).
- Das Gateway wird gelegentlich nicht angehalten, wenn der Befehl 'net stop „Sun Identity Manager Gateway"' verwendet wird (ID-2337).

Aufgaben

- Administratoren mit Identity Manager-Administratorrechten können die Seite zum Verwalten von Aufgaben nicht anzeigen, wenn sich in der Aufgabenliste eine Risikoanalyse befindet (ID-1225).
- Administratoren, die keine Rechte für das oberste Element („Top") besitzen, können keine geplanten Aufgaben für Discovery oder ResourceScanner erstellen (ID-1414).
- Auf der Seite zum Ermitteln von Aufgaben wird die Anzahl der Aufgaben, die den Suchkriterien entsprechen (ID-5152), nicht angezeigt.
- Wenn Sie eine geplante Aufgabe bearbeiten, muss das Startdatum im Format MM/DD/YYYY erneut angegeben werden (ID-5675).

- Delegierte Administratoren, die keine Rechte für das oberste Element („Top“) besitzen, können zwar Aufgaben planen und Aufgabenergebnisse anzeigen, die betreffende Aufgaben nach der Erstellung jedoch nicht anzeigen (ID-6659). Die geplante Aufgabe wurde an oberster Stelle platziert, und der delegierte Administrator ist nicht berechtigt, das Objekt anzuzeigen.
- In der Bibliothek wurde ein Feld für aufgeschobene Aufgaben hinzugefügt, in dem die aufgeschobenen Aufgaben für einen Benutzer aufgeführt sind. Um dieses Feld zu implementieren, müssen Sie zum Benutzerformular und zum Benutzeranzeigeformular, die beide in Registerkarten unterteilt sind, folgende Zeile hinzufügen (ID-7660).

```
<FieldRef name='Deferred Tasks'/>
```

Workflow, Formulare, Regeln und XPRESS

- Die <eq>-Funktion von XPRESS kann nicht zum Vergleich von booleschen Werten mit den Zeichenfolgen TRUE oder FALSE oder den Ganzzahlen 1 oder 2 verwendet werden (ID-3904). Zwischenlösung:

```
<cond>
   <isTrue><ref>Boolesche_Variable</ref></isTrue>
   <s>True action</s>
   <s>False action</s>
</cond>
```

- Pfadausdrücke funktionieren nicht bei der Iteration einer Liste mit generischen Objekten über eine Dolist (ID-4920).

```
<dolist name='genericObj'>
   <ref>listOfGenericObjects</ref>
   <ref>genericObj.name</ref>
</dolist>
```

Zwischenlösung: Verwenden Sie <get> / <set> (siehe unten angegebenes Beispiel):

```
<dolist name='genericObj'>
   <ref>listOfGenericObjects</ref>
   <get><ref>genericObject</ref><s>name</s>
</dolist>
```

- Wenn Sie global.attrname-Variablen für die Felder Ihres Benutzerformulars verwenden und das Attribut für mehrere Ressourcen freigegeben ist, müssen Sie außerdem eine Ableitungsregel definieren (ID-5074). Wenn andernfalls das Attribut nativ auf einer der Ressourcen geändert wird, kann es willkürlich ausgewählt und auf andere Ressourcen übertragen werden.
- In HTML-Komponenten von Formularen können keine Sonderzeichen verwendet werden, die mit & beginnen. So wird beispielsweise   nicht als Leerzeichen dargestellt. Dieses Problem entstand wegen der neuen Unterstützung von Sonderzeichen (&\<>') in Auswahllisten (ID-5548).
- Bei in Formular-, Workflow- und Regelkommentare enthaltenen <Comment>-Tags wird das Zeilenvorschubzeichen durch die Zeichenfolge
 repräsentiert (ID-6243). Diese Zeichen werden für diese Objekte nur im XML-Format angezeigt. Server und Business Process Editor von Identity Manager verarbeiten diese Zeichen korrekt.
- Wenn Sie das Ressourcentabellenbenutzer-Formular zum Bearbeiten von Benutzern verwenden, während Sie die Ressource eines Benutzers bearbeiten, werden die Ressourcenattribute bei der ersten Anzeige des Formulars nicht abgerufen. Zwischenlösung: Klicken Sie auf „Aktualisieren“, um die Attributdaten abzurufen. (ID-10551).

Service Provider Edition

- Identity Manager SPE und Sun Java System Portal Server sind wegen eines Problems in den verschlüsselten Bibliotheken nicht immer kompatibel. (ID-10744).

  Sie können dieses Problem beheben, indem Sie folgende Werte in der Datei `/etc/opt/SUNWam/config/AMConfig.properties` für den Portalserver festlegen und anschließend den Webcontainer neu starten:

  ```
  com.iplanet.security.encryptor=com.iplanet.services.util.JCEEncryption
  com.iplanet.security.SSLSocketFactoryImpl=netscape.ldap.factory.
     JSSESocketFactory
  com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.am.util.
     SecureRandomFactoryImpl
  ```

- Beim Arbeiten mit SPE-Bedienfeldern: Falls das erstmalige Laden der Diagramme mehrere Minuten dauert, sollten Sie sicherstellen, dass der Browser nicht für MSJVM (Microsoft Java Virtual Machine) konfiguriert ist. Identity Manager SPE unterstützt MSJVM nicht für die Ausführung von Browserapplets. (ID-10837).

- Einige Konfigurationsoptionen in der Identity Manager-Administratorbenutzeroberfläche werden in Identity Manager SPE nicht verwendet (ID-10843). Dazu zählen:
  - Ressourcenoptionen: Regeln zum Ausschließen von Konten, Genehmiger, und die Organisation, der eine Ressource zugewiesen ist.
  - Rollenattribute
- Standardmäßig wird die Überwachung bei Aufrufen von `checkinObject`- und `deleteObject` der IDMXContext-API nicht ausgeführt. Die Überwachung ist stets ausdrücklich anzufordern, indem der `IDMXContext.OP_AUDIT`-Schlüssel in der Optionszuordnung, die diesen Methoden übergeben wird, auf TRUE gesetzt wird. Die Methode `createAndLinkUser()` der Klasse „ApiUsage" veranschaulicht, wie die Überwachung anzufordern ist. (ID-11261).
- Beim Aufrüsten von Version 6.0 kann es vorkommen, dass die Hauptkonfigurationsseite der Service Provider Edition Warnungen zu ungültigen Parameters (z.B. SPE: User Directory) anzeigt, obwohl diese Werte in der entsprechenden Dropdown-Liste als gültig erscheinen. Zwischenlösung: Wählen Sie den gleichen Parameterwert ohne Klammern aus der Dropdown-Liste aus und speichern Sie die Konfiguration. (ID-14818).
- Die Standard-Anmeldemodulgruppe von Service Provider erwartet, dass die Ressource „Service Provider" 'SPE End-User Directory' heißt. Wenn diese Ressource einen anderen Namen hat, funktioniert die Service Provider-Seite für die Endbenutzeranmeldung nicht ordnungsgemäß und zeigt keine Anmeldefelder an. (ID-14891).

  Zwischenlösung: Der Ressourcenname „UI_LOGIN_MOD_GRP_DEFAULT_SPE_PWD" des Objekts „LoginModGroup" ist entsprechend zu ändern, sodass er den richtigen Ressourcenname enthält.

Auditor

Administratorbenutzeroberfläche

- Auf der untergeordneten Registerkarte „Abgeschlossen“ der Registerkarte „Korrekturen“ wird bei Auswahl die Farbe nicht geändert. (ID-9149).
- Durch die Gebietsschemaeinstellung des Anwendungsservers kann es sein, dass bei aktivierter Lokalisierung zwei Sprachen angezeigt werden. (ID-9468).

  Zwischenlösung: Wenn Sie den Wert für das Gebietsschema auf „C“ setzen, wird das Problem möglicherweise gelöst.
- Die Hilfeseite für die Seiten „Neue Überprüfungsrichtlinie erstellen“ und „Überprüfungsrichtlinie bearbeiten“ fehlt. (ID-13040).

Überprüfungsrichtlinien

- Während einer Suche wird der erneute Abruf von Benutzerkonten, die von den Ressourcen nicht abgerufen werden konnten oder bei denen andere Ausfälle aufgetreten sind, nicht unterstützt. Diese Ausfälle werden nach dem Abschluss einer Suche gemeldet. Es gibt jedoch keine automatisierte Möglichkeit zur erneuten Prüfung der Konten. (ID-9112).
- Auditor versucht, die Benutzer zwischen Richtlinienprüfungen konform zu halten, indem die Richtlinie immer dann durchgesetzt wird, wenn der Benutzer bearbeitet wird. Wenn Sie einen Benutzer bearbeiten, dem Überwachungsrichtlinien zugewiesen sind und der außerdem eine Richtlinie verletzt, können Sie die Änderungen beim Benutzer nicht speichern, und zwar auch dann nicht, wenn der Benutzer lediglich zu einer anderen Organisation verschoben werden soll. (ID-9504).

  Zwischenlösung: Über das Kontextmenü (oder die Suchfunktion) im Benutzerapplet können Sie Benutzer verschieben oder die Prüfungen der Überwachungsrichtlinie vorübergehend deaktivieren.

  Zum Deaktivieren von Auditorrichtlinien müssen Sie aus der Systemkonfiguration die Eigenschaft `userViewValidators` entfernen. Diese Eigenschaft hat den Wert Zeichenfolgenliste und wird während des Imports von `init.xml` oder `upgrade.xml` hinzugefügt.

- In der grafischen Benutzeroberfläche des Überprüfungsrichtlinienassistenten können 3 Korrekturen und der Zeitraum für zusätzliche Genehmigungen zwischen diesen angegeben werden. Bei Angabe des Zeitraums ist der Korrektor einzugeben, sonst wird die Korrektur gelöscht. (ID-14198).

Berichte

- In den Verstoßverlaufsberichten für AuditPolicy, Ressourcen und Organisationen kann die Implementierung der logarithmischen Skalierung für den Diagrammtyp STACK zu einer ungewöhnlichen Anzeige führen. (ID-9522).
- Das **Konformitätsverletzungsprotokoll für Benutzer** darf in der Dropdown-Liste „Berichte" unter „Auditor-Berichte" nicht angezeigt werden, da dies die Aufgabe für den **Default Compliance Audit Report** ist und verborgen sein muss. (ID-14721)
- Wenn das Formular „Details zum Richtlinienverstoß" in einer früheren Version benutzerspezifisch angepasst wurde, sollten Sie es vor dem Aufrüsten auf Version 7.0 exportieren und das gespeicherte Formular nach dem Aufrüsten wieder importieren. (ID-14772).
- Administratoren für Auditor-Zugriffsabfragen können keine Überwachungsrichtliniensuchen planen. (ID-14713).

  Zwischenlösung: Sie können die Berechtigung zum Erstellen in der Aufgabenplanung zuweisen oder den Bericht mit den Berechtigungen „Auditor-Administrator" oder „Waveset-Administrator" planen.
- Wenn Sie Überprüfungsrichtliniensuchen in früheren Identity Auditor-Versionen erstellt haben, sind diese Berichte nach dem Aufrüsten auf Identity Manager 7.0 nicht mehr sichtbar. Lösung: Ein Administrator mit der Berechtigung „Auditor-Bericht-Administrator" (oder höher) kann diese Berichte bearbeiten und deren Sichtbarkeit auf **run** setzen. (ID-14881).

Regelmäßige Zugriffsprüfungen

- Nach dem Beginn einer regelmäßigen Zugriffsprüfung ist diese erst in der Liste auf der Zugriffsprüfungsseite sichtbar, nachdem Sie auf „Aktualisieren“ geklickt haben. (D-14169)
- Wenn Sie einen Zugriffsprüfungsdetailbericht bearbeiten, in dem das betreffende Zugriffsprüfungsziel gelöscht wurde, wird ein Fehler angezeigt (ID-14805).

  Zwischenlösung: Löschen Sie den Bericht und erstellen Sie einen neuen Bericht.
- Überprüfungsrichtlinienabfragen bzw. Zugriffsprüfungen können nicht ausgeführt werden, wenn der Benutzergültigkeitsbereich auf eine dynamische Organisation gesetzt ist. Dieses Problem tritt aufgrund eines Fehlers im Prüfungscode auf, wo die Regel zur Evaluierung dynamischer Organisationen fehlschlägt, weil das Prüfsubjekt nicht definiert wurde. (ID-14886).

  Zwischenlösung (für Zugriffsprüfungen): Erstellen Sie eine Regel zum Benutzergültigkeitsbereich, die die gleiche Logik verwendet wie die Regel für dynamische Organisationen, und nutzen Sie diese Regel zum Festlegen des Gültigkeitsbereiches für Zugriffsprüfungen.

Arbeitseinheiten

- Beim Weiterleiten einer Bescheinigungs-Arbeitseinheit sind alle vom weiterleitenden Bescheiniger eingegebenen Kommentare in der Arbeitseinheit (Objekt „WorkItem“) enthalten, sodass bei der Endbescheinigung der Arbeitseinheit alle Kommentare von anderen Bescheinigern sichtbar sind. (ID-14643).

Hinweise zur Installation und Aktualisierung

Dieser Abschnitt enthält Informationen zur Installation und Aktualisierung von Identity Manager.

HINWEIS Ausführliche Anweisungen zur Produktinstallation finden Sie in den Dokumenten *Versionshinweise für Sun Java™ System Identity Manager Upgrade* und *Versionshinweise für Sun Java™ System Identity Manager Installation*.

Installationshinweise

Die folgenden Informationen gelten für die Produktinstallation:

- Sie müssen Identity Manager unter HP-UX manuell installieren.
- Das Installationsprogramm von Identity Manager kann jetzt Installationen und Aktualisierungen in beliebigen Installationsverzeichnissen vornehmen. Sie müssen dieses Verzeichnis vor dem Installationsvorgang erstellen oder ein Verzeichnis aus dem Setup-Fenster auswählen.
- Zur Ausführung von Identity Manager unter Tomcat 4.1.*x* müssen Sie die JSSE Jar-Dateien von der Sun-Website `http://java.sun.com/products/jsse/index-103.html` herunterladen und diese in das Verzeichnis `idm\WEB-INF\lib` kopieren.
- Zur Ausführung von Sun Identity Manager Gateway unter Windows NT muss das Zusatzmodul Microsoft Active Directory Client installiert sein. Den DSClient finden Sie auf der folgenden Internetadresse:

  `http://support.microsoft.com/default.aspx?scid=kb;en-us;Q288358`

Hinweise zur Aufrüstung

Dieser Abschnitt enthält eine Zusammenfassung der Aufgaben, die Sie zum Aufrüsten von Identity Manager von Version 6.0 Version 7.0 ausführen müssen. Informationen darüber, welche Versionen auf Identity Manager 7.0 aufgerüstet werden können, finden Sie in „Aufrüstungsmöglichkeiten für Identity Manager“ auf Seite 13.

Ausführliche Informationen und Anweisungen finden Sei unter *Versionshinweise für Sun Java™ System Identity Manager Aufrüstung*.

HINWEIS

- Vor dem Aufrüsten von Identity Manager sollten Sie in der Installationsanleitung für Ihren Anwendungsserver in *Versionshinweise für Sun Java™ System Identity Manager Installation* nach anwendungsserverspezifischen Anweisungen suchen.
- Wenn für Ihre aktuelle Identity Manager-Installation viele individuelle Anpassungen erforderlich sind, sollten Sie sich mit Sun Professional Services in Verbindung setzen, die Sie bei der Planung und Ausführung der Aufrüstung unterstützen.
- Beim Aufrüsten mit JDK 1.4 kann während dieses Vorgangs ein Ausnahmefehler auftreten. (ID-14258)

  Zwischenlösung:

  Führen Sie die Aufrüstung mithilfe des grafischen Installationsprogramms durch

  oder

  (bei Verwendung des textbasierten Installationsprogramms) Fügen Sie zum Installationsskript „`-Djava.awt.headless=true`" wie folgt hinzu:

  ```
  if [ -n "$WS_DEBUG" ]; then
  FLAGS="$FLAGS -Dwaveset.debug=$WS_DEBUG"
  fi
  FLAGS="$FLAGS -Djava.awt.headless=true"
  ```

Arbeiten mit Aufrüstungsprogramm von Identity Manager

Dieser Abschnitt enthält die Schritte zum Aufrüsten von Identity Manager mithilfe des Installations- und Aufrüstungsprogramms von Identity Manager.

HINWEIS

- Die meisten Hauptversionen von Identity Manager nutzen neue Schemen. Vor dem Aufrüsten auf die neue Version von Identity Manager müssen Sie Ihr Schema aktualisieren.
- In einigen Umgebungen (wie z.B. HP-UX) kann es sein, dass Sie die alternative (manuelle) Aktualisierung durchführen müssen. Falls dies der Fall ist, fahren Sie mit „Manuelle Aufrüstung“ auf Seite 70 fort.
- In UNIX-Umgebungen müssen Sie sich vergewissern, dass das Verzeichnis `/var/opt/sun/install` existiert und nicht schreibgeschützt ist.
- Während der Aktualiserung werden Sie gefragt, in welchem Verzeichnis Ihr Anwendungsserver installiert ist
- Alle vorher installierten Hotfixes werden im folgenden Verzeichnis archiviert:

  `$WSHOME/patches/`*`HotfixName`*
- Die in den folgenden Schritten angegebenen Befehle gelten für eine Windows-Installation und einen Tomcat-Anwendungsserver. Je nach Umgebung können sich die von Ihnen zu verwendenden Befehle von den hier angegebenen unterscheiden.

So rüsten Sie Identity Manager auf:

1. Fahren Sie den Anwendungsserver herunter.
2. Bei einer Aufrüstung auf Identity Manager *6.0* oder Identity Manager *7.0* müssen Sie das Schema der Repository-Datenbank wie folgt aufrüsten:
   - Ab **Identity Manager 6.0** wird ein Schema verwendet, das neue Tabellen für Aufgaben, Gruppen und Organisationen sowie die syslog-Tabelle enthält. Sie müssen diese neuen Tabellen erstellen und ihre vorhandenen Daten in diese Tabellen kopieren.
   - Identity Manager 6.0 speichert Objekte in zwei Tabellen. Sie können zum Ändern von Schemen die im Verzeichnis `db_scripts` befindlichen Beispiel-Skripten nutzen. Zum Aufrüsten der Repository-Tabellen dient das Skript `db_scripts/upgradeto2005Q4M3.`*Datenbankname*.

   HINWEIS

   - Vor dem Aufrüsten des Repository-Schemas sollten Sie von allen Repository-Tabellen Sicherungskopien erstellen.
   - Die Aufrüstung von MySQL-Datenbanken ist ziemlich kompliziert. Weitere Informationen finden Sie in `db_scripts/upgradeto2005Q4M3.mysql`.

- **Identity Manager 7.0** führt neue Tabellen für Benutzeransprüche (UserEntitlement-Objekte) ein.
  Sie müssen diese neuen Tabellen erstellen und ihre vorhandenen Daten in diese Tabellen kopieren. Sie können zum Ändern von Schemen die im Verzeichnis `db_scripts` befindlichen Beispiel-Skripten nutzen.

HINWEIS	• Vor dem Aufrüsten des Repository-Schemas sollten Sie von allen Repository-Tabellen Sicherungskopien erstellen. • Weitere Informationen hierzu finden Sie im Skript `db_scripts/upgrade7.0.`*DBMSName*.

3. Wenn in Ihrem System das Sun Identity Manager Gateway auf dem Identity Manager-Server ausgeführt wird, können Sie den Gateway-Dient mit dem folgenden Befehl herunterfahren:

```
net stop "Sun Identity Manager Gateway"
```

4. Wählen Sie eine der folgenden Verfahren, um das Installationsprogramm zu starten:
   - Zum Aufrufen des Installationsprogramms mit grafischer Benutzeroberfläche müssen Sie `install.bat` (Windows) bzw. `install` (UNIX) ausführen.

     Das Installationsprogramm zeigt ein Begrüßungsfenster an.
   - Zum Umschalten des Installationsprogramms in den `nodisplay`-Modus müssen Sie in das Verzeichnis wechseln, in dem sich die Software befindet, und dann den folgenden Befehl eingeben:

     ```
     install -nodisplay
     ```

     Das Installationsprogramm zeigt den Begrüßungstext an und stellt Ihnen dann eine Reihe von Fragen, um Installationsinformationen in der gleichen Reihenfolge wie das grafische Installationsprogramm abzufragen.

HINWEIS	• Wenn das System keinen Monitor besitzt, schaltet das Installationsprogramm standardmäßig in den `nodisplay`-Modus. • Das Installationsprogramm installiert niemals eine ältere über einer neueren Softwareversion. In einer solchen Situation wird eine Fehlermeldung angezeigt und das Installationsprogramm wird beendet.

5. Klicken Sie im Begrüßungsfenster auf „Weiter“.
6. Wählen Sie im Fenster „Install or Upgrade?“ die Option „Upgrade“ und klicken Sie dann auf „Weiter“.

7. Wählen Sie im Fenster „Select Installation Directory“ das Verzeichnis, in dem sich die frühere Identity Manager-Version befindet, und klicken Sie dann auf „Weiter“.

   Das Installationsprogramm zeigt für Vorgänge vor und nach der Aufrüstung Verlaufsleisten an und öffnet dann das Fenster „Installation Summary“.

8. Ausführliche Informationen zur Installation erhalten Sie, indem Sie auf auf „Details“ klicken, die Protokolldatei anzeigen und danach auf „Schließen“ klicken, um das Installationsprogramm zu beenden.

9. Entfernen Sie alle compilierten Identity Manager-Dateien aus dem Arbeitsverzeichnis des Anwendungsservers.

10. Wenn das Gateway auf einem anderen, über Netzwerk zugänglichen System ausgeführt wird, müssen Sie es wie folgt aufrüsten.

    a. Melden Sie sich im Windows-System an und wechseln Sie in das Verzeichnis, in dem das Gateway installiert ist.

    b. Fahren Sie den Gateway-Dienst durch Eingeben des folgenden Befehls herunter:

    ```
    gateway -k
    ```

    c. Bei Windows 2000-Systemen (oder neueren Betriebssystemversionen) müssen Sie alle Instanzen des MMC-Plugins „Dienste“ beenden.

    d. Geben Sie den folgenden Befehl ein, um den Gateway-Dienst zu entfernen:

    ```
    gateway -r
    ```

    e. Machen Sie von den vorhandenen Gateway-Dateien Sicherungskopien und löschen Sie diese danach.

    f. Entpacken Sie die neuen Gateway-Dateien.

       Wenn Sie das neu aufgerüstete Gateway auf einem System installieren, auf dem nicht der Identity Manager-Server läuft müssen Sie die Datei `gateway.zip` von der Installations-CD von Identity Manager kopieren.

    g. Entpacken Sie die Datei `gateway.zip` in das Verzeichnis, in dem das Gateway installiert war.

    h. Geben Sie den folgenden Befehl ein, um den Gateway-Dienst zu installieren:

    ```
    gateway -i
    ```

    i. Geben Sie den folgenden Befehl ein, um den Gateway-Dienst zu starten:

    ```
    gateway -s
    ```

Manuelle Aufrüstung

In einigen Umgebungen kann es sein, dass Sie die Aufrüstung manuell durchführen müssen und dafür nicht das Installations- und Aufrüstungsprogramm von Identity Manager verwenden können.

HINWEIS

- Vergewissern Sie sich, dass die Umgebungsvariable `JAVA_HOME` gesetzt ist.
- Stellen Sie sicher, dass sich das Verzeichnis `bin` im Verzeichnis `JAVA_HOME` im Pfad befindet.
- Alle vorher installierten Hotfixes werden im Verzeichnis `$WSHOME/patches/`*HotfixName* archiviert:

Windows-Plattform

Gehen Sie wie folgt vor, um Identity Manager manuell auf einer unterstützten Windows-Plattform aufzurüsten:

1. Fahren Sie den Anwendungsserver und das Sun Identity Manager Gateway herunter.
2. Aktualiseren Sie die Identity Manager-Datenbank (ausführliche Anweisungen dazu finden Sie in Schritt 2 auf Seite 67).
3. Geben Sie die folgenden Befehle ein, um die Umgebungsvariablen entsprechend zu setzen:

   ```
   set ISPATH=Pfad, in den die Software installiert werden soll
   set WSHOME=Pfad zum Installations- ODER Staging-Verzeichnis von Identity Manager
   set TEMP=Pfad zum temporären Verzeichnis
   ```

4. Ausführen der Vorverarbeitung:

   ```
   mkdir %TEMP%
   cd /d %TEMP%
   jar -xvf %ISPATH%\IDM.WAR \
   WEB-INF\lib\idm.jar WEB-INF\lib\idmcommon.jar
   set TMPLIBPTH=%TEMP%\WEB-INF\lib
   set CLASSPATH=%TMPLIBPTH%\idm.jar;\
   %TMPLIBPTH%\idmcommon.jar;
   java -classpath %CLASSPATH% -Dwaveset.home=%WSHOME% \
      com.waveset.install.UpgradePreProcess
   ```

5. Software-Installation:

   ```
   cd %WSHOME%
   jar -xvf %ISPATH%\IDM.WAR
   ```

6. Ausführen der Nachverarbeitung:

```
java -classpath %CLASSPATH% -Dwaveset.home=%WSHOME%
  com.waveset.install.UpgradePostProcess
```

HINWEIS Das Installationsprogramm unterstützt die Aufrüstung von Installationen, die das Konfigurator-Standardkonto umbenannt, gelöscht oder deaktiviert haben.

Das Installationsprogramm fordert Sie zur Eingabe des Benutzernamens und des Passworts auf, damit die Datei `update.xml` während der Nachverarbeitung des Aufrüstungsvorgangs importiert werden kann. Wenn der Benutzername oder das Passwort falsch eingegeben wurden, haben Sie maximal drei Versuche, das richtige Passwort einzugeben. Der Fehler wird im Textfeld dahinter angezeigt.

Bei der manuellen Installation müssen Sie die Flags `-U` *Benutzername* `-P` *Passwort* angeben, damit die Berechtigungsnachweise an die Prozedur `UpgradePostProcess` übergeben werden können.

---

7. Bei der Installation in ein Staging-Verzeichnis müssen Sie für das Deployment in Ihrem Anwendungsserver eine `.war`-Datei erstellen.
8. Entfernen Sie die Identity Manager-Dateien aus dem Arbeitsverzeichnis des Anwendungsservers.
9. Verlagern Sie eventuell vorhandene Hotfix-Klassendateien aus dem Verzeichnis `WEB-INF\classes` in das Verzeichnis `$WSHOME\patches\`*HotfixName*, falls das der Aufrüstungsvorgang nicht bereits erledigt hat.
10. Starten Sie den Anwendungsserver.
11. Rüsten Sie Sun Identity Manager Gateway auf und starten Sie ihn dann neu (ausführliche Anweisungen dazu finden Sie in Schritt 10 auf Seite 69).

Unix-Plattform

Gehen Sie wie folgt vor, um Identity Manager manuell auf einer unterstützten Unix-Plattform aufzurüsten:

1. Fahren Sie den Anwendungsserver und das Sun Identity Manager Gateway herunter.
2. Aktualiseren Sie die Identity Manager-Datenbank (Anweisungen dazu finden Sie in Schritt 2 auf Seite 67).
3. Geben Sie die folgenden Befehle ein, um die Umgebungsvariablen entsprechend zu setzen:

```
export ISPATH=Pfad, in den die Software installiert werden soll
export WSHOME=Pfad zum Installations- ODER Staging-Verzeichnis von Identity Manager
export TEMP=Pfad zum temporären Verzeichnis
```

4. Ausführen der Vorverarbeitung:

```
mkdir $TEMP
cd $TEMP
jar -xvf $ISPATH/idm.war \
WEB-INF/lib/idm.jar WEB-INF/lib/idmcommon.jar
CLASSPATH=$TEMP/WEB-INF/lib/idm.jar:\
$TEMP/WEB-INF/lib/idmcommon.jar:
java -classpath $CLASSPATH -Dwaveset.home=$WSHOME \
com.waveset.install.UpgradePreProcess
```

5. Software-Installation:

```
cd $WSHOME
jar -xvf $ISPATH/idm.war
```

6. Run post-process:

```
java -classpath $CLASSPATH -Dwaveset.home=$WSHOME
  com.waveset.install.UpgradePostProcess
```

HINWEIS Das Installationsprogramm unterstützt die Aufrüstung von Installationen, die das Konfigurator-Standardkonto umbenannt, gelöscht oder deaktiviert haben.

Das Installationsprogramm fordert Sie zur Eingabe des Benutzernamens und des Passworts auf, damit die Datei `update.xml` während der Nachverarbeitung des Aufrüstungsvorgangs importiert werden kann. Wenn der Benutzername oder das Passwort falsch eingegeben wurden, haben Sie maximal drei Versuche, das richtige Passwort einzugeben. Der Fehler wird im Textfeld dahinter angezeigt.

Bei der manuellen Installation müssen Sie die Flags `-U` *Benutzername* `-P` *Passwort* angeben, damit die Berechtigungsnachweise an die Prozedur `UpgradePostProcess` übergeben werden können.

---

7. Wechseln Sie in das Verzeichnis `$WSHOME/bin/solaris` bzw. `$WSHOME/bin/linux` und setzen Sie dann für die Dateien im Verzeichnis die Zugriffsrechte so, dass sie ausführbar sind.
8. Bei der Installation in ein Staging-Verzeichnis müssen Sie für das Deployment in Ihrem Anwendungsserver eine `.war`-Datei erstellen.
9. Entfernen Sie die Identity Manager-Dateien aus dem Arbeitsverzeichnis des Anwendungsservers.
10. Verlagern Sie eventuell vorhandene Hotfix-Klassendateien aus dem Verzeichnis `WEB-INF/classes` in das Verzeichnis `$WSHOME/patches/`*HotfixName*, falls das der Aufrüstungsvorgang nicht bereits erledigt hat.
11. Starten Sie den Anwendungsserver.
12. Rüsten Sie Sun Identity Manager Gateway auf und starten Sie ihn dann neu (Anweisungen dazu finden Sie in Schritt 10 auf Seite 69).

Verworfene APIs

Dieses Kapitel enthält alle Identity Manager-APIs (Application Programming Interfaces), die in Identity Manager 6.0 2005Q4M3 verworfen wurden. Außerdem werden, falls verfügbar, deren Nachfolger aufgelistet. Dieses Kapitel ist in folgende Abschnitte unterteilt:

Verworfene Konstruktoren

Die folgende Tabelle enthält die verworfenen Konstruktoren und, falls verfügbar, deren Nachfolger.

Verworfener Konstruktor	Nachfolger
com.sun.idm.idmx.IDMXContext	com.waveset.object.LighthouseContext
com.sun.idm.idmx.IDMXContextFactory	com.waveset.session.SessionFactory
com.waveset.adapter.ActiveDirectoryActiveSyncAdapter	com.waveset.adapter.ADSIResourceAdapter
com.waveset.adapter.AD_LDAPResourceAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.AttrParse	com.waveset.object.AttrParse
com.waveset.adapter.ConfirmedSync	
com.waveset.adapter.DblBufIterator	com.waveset.util.BufferedIterator com.waveset.util.BlockIterator com.waveset.adapter.AccountIteratorWrapper
com.waveset.adapter.DominoActiveSyncAdapter	com.waveset.adapter.DominoResourceAdapter
com.waveset.adapter.LDAPChangeLogActiveSyncAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.NDSActiveSyncAdapter	com.waveset.adapter.NDSResourceAdapter
com.waveset.adapter.PeopleSoftResourceAdapter	
com.waveset.adapter.RemedyActiveSyncResourceAdapter	com.waveset.adapter.RemedyResourceAdapter

Verworfener Konstruktor	Nachfolger
com.waveset.adapter.TopSecretActiveSyncAdapter	com.waveset.adapter.TopSecretResourceAdapter
com.waveset.exception.ConfigurationError	com.waveset.util.ConfigurationError
com.waveset.exception.IOException	com.waveset.util.IOException
com.waveset.exception.XmlParseException	com.waveset.util.XmlParseException
com.waveset.object.IAPI	com.waveset.adapter.iapi.IAPI
com.waveset.object.IAPIProcess	com.waveset.adapter.iapi.IAPIFactory
com.waveset.object.IAPIUser	com.waveset.adapter.iapi.IAPIUser
com.waveset.object.RemedyTemplate	
com.waveset.object.ReportCounter	
com.waveset.object.SourceManager	com.waveset.view.SourceAdapterManageView
com.waveset.security.authn.LoginInfo	com.waveset.object.LoginInfo
com.waveset.security.authn.SignedString	com.waveset.util.SignedString
com.waveset.security.authn.Subject	com.waveset.object.Subject
com.waveset.security.authz.Permission	com.waveset.object.Permission
com.waveset.security.authz.Right	com.waveset.object.Right
com.waveset.util.Debug	com.sun.idm.logging.Trace
com.waveset.util.HtmlUtil	com.waveset.ui.util.html.HtmlUtil
com.waveset.util.ITrace	com.sun.idm.logging.Trace

Verworfene Methoden und Felder

Die Tabellen in diesem Abschnitt enthalten alle Methoden und Felder, die in dieser Version verworfen wurden. Die Methoden und Felder sind nach Klassennamen sortiert.

Die Daten in der Spalte **Nachfolger** können folgende Informationsarten enthalten:

- Wenn die Spalte leer ist, gibt es keinen Nachfolger für die Methode oder das Feld.
- Wenn kein Klassenname angegeben ist, wird der Nachfolger für die Methode oder das Feld in derselben Klasse wie das verworfene Element definiert.
- Wenn der Nachfolger für die Methode oder das Feld in einer anderen Klasse als das verworfene Element definiert ist, wird der Nachfolger in der Javadoc-Syntax aufgelistet. Beispiel: Die `getBaseContextAttrName()`-Methode der Klasse `com.waveset.adapter.ADSIResourceAdapter` wurde verworfen. Der Nachfolger wird als `com.waveset.adapter.ResourceAdapter#ResourceAdapter()` aufgeführt.

  wobei gilt:

  - `com.waveset.adapter` ist der Package-Name.
  - `ResourceAdapter` ist der Klassenname.
  - `ResourceAdapter()` ist die Methode und Argumentliste.

com.waveset.adapter.AccessManagerResourceAdapter

Verworfene Methode	Nachfolger
handlePDException(Exception)	handlePDException(PDException)

com.waveset.adapter.ACF2ResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.ActiveSync

Verworfene Methode	Nachfolger
RA_UPDATE_IF_DELETE	

com.waveset.adapter.ActiveSyncUtil

Verworfene Methode	Nachfolger
getLogFileFullPath()	

com.waveset.adapter.ADSIResourceAdapter

Verworfene Methode	Nachfolger
buildEvent(UpdateRow)	com.waveset.adapter.iapi.IAPIFactory#getIAPI(Map, Map,ResourceAdapterBase)
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBase Contexts()
RA_UPDATE_IF_DELETE	com.waveset.adapter.ActiveSync#RA_DELETE_RULE

com.waveset.adapter.AgentResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.AIXResourceAdapter.BlockAcctIter

Verworfene Methode	Nachfolger
BlockAcctIter(AIXResourceAdapter,CaptureList)	BlockAcctIter(CaptureList)
BlockAcctIter(int,CaptureList)	BlockAcctIter(CaptureList)

com.waveset.adapter.AuthSSOResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.ClearTrustResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.DatabaseTableResourceAdapter

Verworfene Methode	Nachfolger
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

com.waveset.adapter.DB2ResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.DominoResourceAdapter

Verworfene Methode	Nachfolger
buildEvent(UpdateRow)	com.waveset.adapter.iapi.IAPIFactory#getIAPI(Map, Map,ResourceAdapterBase)
RA_UPDATE_IF_DELETE	com.waveset.adapter.ActiveSync#RA_DELETE_RULE

com.waveset.adapter.DominoResourceAdapterBase

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.ExampleTableResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.GenericScriptResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.GetAccessResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.HostConnectionPool

Verworfene Methode	Nachfolger
getConnection(HostAccessLogin)	com.waveset.adapter.HostConnPool#getAffinity Connection(HostAccessLogin)
releaseConnection(HostAccess)	com.waveset.adapter.HostConnPool#releaseConnection (HostAccess)

com.waveset.adapter.HostConnPool

Verworfene Methode	Nachfolger
getConnection(HostAccessLogin)	getAffinityConnection(HostAccessLogin)
putFree()	

com.waveset.adapter.iapi.IAPIFactory

Verworfene Methode	Nachfolger
getIAPIProcess(Map,Map,String,Resource)	getIAPI(Map,Map,String,ResourceAdapterBase)
getIAPIProcess(Element)	
getIAPIUser(Element)	
getIAPIUser(Map,Map,String,Map)	getIAPI(Map,Map,String,ResourceAdapterBase)
getIAPIUser(Map,Map,String,Resource)	getIAPI(Map,Map,String,ResourceAdapterBase)

com.waveset.adapter.IDMResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.INISafeNexessResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.LDAPResourceAdapterBase

Verworfene Methode	Nachfolger
addUserToGroup(LDAPObject,String,String)	addUserToGroup(String,String,String)
buildBaseUrl()	
buildBaseUrl(String)	
buildEvent(UpdateRow)	
getAccountAttributes(String)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()
getGroups(Name,String,Vector,Vector)	getGroups(String,String,Vector,Vector)
getLDAPAttributes(String,DirContext[],String)	getLDAPAttributes(String,DirContext,String,String[])
getLDAPAttributes(String,DirContext[])	getLDAPAttributes(String,DirContext,String,String[])
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE
removeNameFromAttribute(DirContext,Name,Attribute)	removeNameFromAttribute(DirContext,String,boolean,Attribute)
removeUserFromAllGroups(Name,String,WavesetResult)	removeUserFromAllGroups(String,boolean,String,WavesetResult)
removeUserFromGroup(DirContext,Name,String,String,Attributes)	removeUserFromGroup(DirContext,String,boolean,String,String,Attributes)
removeUserFromGroups(Name,Vector,String,WavesetResult)	removeUserFromGroups(String,boolean,Vector,String,WavesetResult)

com.waveset.adapter.MySQLResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.NaturalResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.NDSResourceAdapter

Verworfene Methode	Nachfolger
buildEvent(UpdateRow)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBase Contexts()

com.waveset.adapter.ONTDirectorySmartResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.OS400ResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter

Verworfene Methode	Nachfolger
DEFAULT_AUDIT_STAMP_FORMAT	
DEFAULT_AUDIT_STAMP_START_DATE	
getAccountAttributes(String)	
getUpdateRows(UpdateRow)	getUpdateRows(UpdateRow)
RA_AUDIT_STAMP_FORMAT	

com.waveset.adapter.RACFResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.RASecureConnection

Verworfene Methode	Nachfolger
ExchangeAuth(boolean)	ExchangeAuth(boolean,byte[])

com.waveset.adapter.RedHatLinuxResourceAdapter.BlockAcctIter

Verworfene Methode	Nachfolger
BlockAcctIter(int,CaptureList)	BlockAcctIter(SVIDResourceAdapter,CaptureList)

com.waveset.adapter.RequestResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.ResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

com.waveset.adapter.ResourceAdapterBase

Verworfene Methode	Nachfolger
getAccountAttributes(String)	
getAdapter(Resource,LighthouseContext)	getAdapterProxy(Resource,LighthouseContext)
getAdapter(Resource,ObjectCache,WSUser)	getAdapterProxy(Resource,ObjectCache)
getAdapter(Resource,ObjectCache)	getAdapterProxy(Resource,LighthouseContext)
getBaseContextAttrName()	getBaseContexts()
isExcludedAccount(String,Rule)	com.waveset.adapter.ResourceAdapterProxy#isExcludedAccount(String, Map,ResourceOperation,Rule)
isExcludedAccount(String)	com.waveset.adapter.ResourceAdapterProxy#isExcludedAccount(String, Map,ResourceOperation,Rule)

com.waveset.adapter.ResourceAdapterProxy

Verworfene Methode	Nachfolger
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

com.waveset.adapter.ResourceManager

Verworfene Methode	Nachfolger
getResourceTypes()	getResourcePrototypes() getResourcePrototypes(ObjectCache,boolean)
getResourceTypeStrings()	getResourcePrototypeNames(ObjectCache)

com.waveset.adapter.SAPHRActiveSyncAdapter

Verworfene Methode	Nachfolger
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

com.waveset.adapter.SAPResourceAdapter

Verworfene Methode	Nachfolger
unexpirePassword(String,WavesetResult)	unexpirePassword(String, String,String,WavesetResult)
unexpirePassword(WSUser,WavesetResult)	unexpirePassword(String, String,String,WavesetResult)

com.waveset.adapter.ScriptedConnection

Unterklasse	Verworfene Methode	Nachfolger
Skript	hasNextToken()	
Skript	nextToken()	
ScriptedConnection	disConnect()	com.waveset.adapter.ResourceConnection# disconnect()
ScriptedConnection Factory	getScriptedConnection(String,Hash Map)	com.waveset.adapter.ScriptedConnectionPool# getConnection(HashMap,String,long,boolean)
SSHConnection	disConnect()	disconnect()
TelnetConnection	disConnect()	disconnect()

com.waveset.adapter.ScriptedHostResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.SkeletonResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.SMEResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.SQLServerResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.SunAccessManagerResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()

com.waveset.adapter.SVIDResourceAdapter.BlockAcctIter

Verworfene Methode	Nachfolger
BlockAcctIter(int,CaptureList)	BlockAcctIter(CaptureList)
BlockAcctIter(SVIDResourceAdapter,CaptureList)	BlockAcctIter(CaptureList)

com.waveset.adapter.SybaseResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.TestResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.TopSecretResourceAdapter

Verworfene Methode	Nachfolger
hasError(String,String)	hasError(String,String,String)
login(HostAccess hostAccess)	login(HostAccess,ServerAffinity)

com.waveset.adapter.VerityResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.adapter.XMLResourceAdapter

Verworfene Methode	Nachfolger
getAccountAttributes(String)	

com.waveset.msgcat.Catalog

Verworfene Methode	Nachfolger
getMessage(String,Object[],Locale)	format (Locale,String,Object[])
getMessage(Locale,String,Object[])	format (Locale,String,Object[])
getMessage(Locale,String)	format (Locale,String)
getMessage(String,Locale)	format (Locale,String)
getMessage(String,Object[])	format (Locale,String,Object[])

com.waveset.object.Account

Verworfene Methode	Nachfolger
getUnowned()	hasOwner()
setUnowned(boolean)	setOwner(WSUser)

com.waveset.object.AccountAttributeType

Verworfene Methode	Nachfolger
getAttrType()	getSyntax()
setAttrType(String)	setSyntax(String) setSyntax(Syntax)

com.waveset.object.Attribute

Verworfene Methode	Nachfolger
BLOCK_SIZE	BLOCK_ROWS_GET BLOCK_ROWS_LIST
EVENTDATE	EVENT_DATETIME
EVENTTIME	EVENT_DATETIME
getDbColumnLength()	
getDbColumnName()	
STARTUP_TYPE_AUTO	com.waveset.object.Resource#STARTUP_TYPE_AUTO
STARTUP_TYPE_AUTO_FAILOVER	com.waveset.object.Resource#STARTUP_TYPE_AUTO_FAILOVER
STARTUP_TYPE_DISABLED	com.waveset.object.Resource#STARTUP_TYPE_DISABLED
STARTUP_TYPE_MANUAL	com.waveset.object.Resource#STARTUP_TYPE_MANUAL
STARTUP_TYPES	com.waveset.object.Resource#STARTUP_TYPES
STARTUP_TYPES_DISPLAY_NAMES	com.waveset.object.Resource#STARTUP_TYPES_DISPLAY_NAMES

com.waveset.object.AttributeDefinition

Verworfene Methode	Nachfolger
AttributeDefinition(String,String)	AttributeDefinition(String,Syntax)
setAttrType(String)	setSyntax(Syntax)

com.waveset.object.AuditEvent

Verworfene Methode	Nachfolger
setAttributeMap(Map)	setAuditableAttributes(Map)
addAuditableAttributes(AccountAttributeType[], WSAttributes)	setAuditableAttributes(Map)
getAttributeMap()	getAuditableAttributes()
getAttributeValue(String)	getAuditableAttributes()
setAccountAttributesBlob(Map)	setAccountAttributesBlob(Map,Map)
setAccountAttributesBlob(WSAttributes,List)	setAccountAttributesBlob(WSAttributes,WSAttributes, List)

com.waveset.object.CacheManager

Verworfene Methode	Nachfolger
getAllObjects(Type,AttributeCondition[])	listObjects(Type,AttributeCondition[])
getAllObjects(Type,WSAttributes)	listObjects(Type,WSAttributes)
getAllObjects(Type)	listObjects(Type)

com.waveset.object.Constants

Verworfene Methode	Nachfolger
MAX_SUMMARY_STRING_LENGTH	

com.waveset.object.EmailTemplate

Verworfene Methode	Nachfolger
setToAddress(String)	setTo(String)
getFromAddress()	getFrom()
getToAddress()	getTo()
setFromAddress(String)	setFrom(String)
VAR_FROM_ADDRESS	VAR_FROM
VAR_TO_ADDRESS	VAR_TO

com.waveset.object.Form

Verworfene Methode	Nachfolger
EL_HELP	com.waveset.object.GenericObject#toMap(int)
getDefaultDataType()	getDefaultSyntax()
getType()	getSyntax()
setType(String)	setSyntax(Syntax)

com.waveset.object.GenericObject

Verworfene Methode	Nachfolger
toMap(boolean)	toMap(String,int)
toMap(String,boolean)	

com.waveset.object.LoginConfig

Verworfene Methode	Nachfolger
getApp(String)	getLoginApp(String)

com.waveset.object.MessageUtil

Verworfene Methode	Nachfolger
getActionDisplayKey(String)	
getEventParmDisplayKey(String)	
getResultDisplayKey(String)	
getTypeDisplayKey(String)	com.waveset.ui.FormUtil#getTypeDisplayName (LighthouseContext,String)

com.waveset.object.RepositoryResult

Verworfene Methode	Nachfolger
get(int)	
getId(int)	
getName(int)	
getObject(int)	
getRowCount()	
getRows()	
seek(int)	hasNext() next()
sort()	

com.waveset.object.RepositoryResult.Row

Verworfene Methode	Nachfolger
getSummaryAttributes()	getAttributes()

com.waveset.object.ResourceAttribute

Verworfene Methode	Nachfolger
setType(String)	setSyntax(Syntax)

com.waveset.object.TaskInstance

Verworfene Methode	Nachfolger
DATE_FORMAT	com.waveset.util.Util#stringToDate(String,String) com.waveset.util.Util#getCanonicalDate(Date) com.waveset.util.Util#getCanonicalDate(Date,TimeZone) com.waveset.util.Util#getCanonicalDate(long)
VAR_RESULT_LIMIT	setResultLimit(int) getResultLimit()
VAR_TASK_STATUS	

com.waveset.object.TaskTemplate

Verworfene Methode	Nachfolger
setMode(String)	setExecMode(String)
setMode(TaskDefinition.ExecMode)	setExecMode(TaskDefinition,ExecMode)

com.waveset.object.Type

Verworfene Methode	Nachfolger
AUDIT_CONFIG	
AUDIT_PRUNER_TASK	
AUDIT_QUERY	
DISCOVERY	
getSubtypes()	getLegacyTypes()
NOTIFY_CONFIG	

Verworfene Methode	Nachfolger
REPORT_COUNTER	
SUMMARY_REPORT_TASK	
USAGE_REPORT	
USAGE_REPORT_TASK	

com.waveset.object.UserUIConfig

Verworfene Methode	Nachfolger
getCapabilityGroups()	
getAppletColumns()	getAppletColumnDefs()
getCapabilityGroup(String)	
getCapabilityGroupNames()	
getFindMatchOperatorDisplayNameKeys()	
getFindMatchOperators()	
getFindResultsColumns()	
getFindResultsSortColumn()	
getFindUserDefaultSearchAttribute()	
getFindUserSearchAttributes()	
getFindUserShowAttribute(int)	
getFindUserShowCapabilitiesSearch(int)	
getFindUserShowDisabled(int)	
getFindUserShowOrganizationSearch(int)	
getFindUserShowProvisioningSearch(int)	
getFindUserShowResourcesSearch(int)	
getFindUserShowRoleSearch(int)	

com.waveset.object.ViewMaster

Verworfene Methode	Nachfolger
ViewMaster()	ViewMaster(LighthouseContext)
ViewMaster(String,String)	ViewMaster(LighthouseContext)
ViewMaster(Subject,String)	ViewMaster(LighthouseContext)

com.waveset.session

Unterklasse	Verworfene Methoden oder Felder	Nachfolger
Sitzung	listApprovers()	getAdministrators(Map)
	listControlledApprovers()	getAdministrators(Map)
	listSimilarApprovers(String adminName)	getAdministrators(Map)
SessionFactory	getApp(String)	getLoginApp(String)
	getApps()	getLoginApps()
WorkflowServices	ARG_TASK_DATE	com.waveset.object.Attribute#DATE

com.waveset.task.TaskContext

Verworfene Methode	Nachfolger
getAccessPolicy()	
getRepository()	

com.waveset.ui.util.FormUtil

Verworfene Methode	Nachfolger
getAdministrators(Session,List)	getUsers(LighthouseContext,Map)
getAdministrators(Session,Map)	getUsers(LighthouseContext,Map)
getApplications(LighthouseContext,List)	getApplications(LighthouseContext,Map)
getApplications(LighthouseContext)	getApplications(LighthouseContext,Map)

Verworfene Methode	Nachfolger
getApproverNames(Session,List)	getUsers(LighthouseContext,Map)
getApproverNames(Session)	getUsers(LighthouseContext,Map)
getApprovers(Session,List)	getUsers(LighthouseContext,Map)
getApprovers(Session)	getUsers(LighthouseContext,Map)
getCapabilities(LighthouseContext,List,Map)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext,List)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext,String,String)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext)	getCapabilities(LighthouseContext,Map)
getObjectNames(LighthouseContext,String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,List)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,String, String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,String,String, List)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,Type,String,String, List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,Type,String,String, List)	getObjectNames(LighthouseContext,String,Map)
getOrganizations(LighthouseContext,boolean,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizations(LighthouseContext,boolean)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizations(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizations(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext, boolean,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext, boolean)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNamesWithPrefixes(Lighthouse Context,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNamesWithPrefixes(Lighthouse Context)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getSimilarApproverNames(Session,String)	getUsers(LighthouseContext,Map)

Verworfene Methode	Nachfolger
getSimilarApproverNames(Session)	getUsers(LighthouseContext,Map)
getUnassignedOrganizations(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizations(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext,Map)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNamesWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNamesWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,List,List)	getUnassignedResources(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,String,List)	getUnassignedResources(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,String)	getUnassignedResources(LighthouseContext,Map)

com.waveset.ui.util.html

Unterklasse	Verworfene Methode	Nachfolger
Komponente	isNoWrap()	
	setHelpKey(String)	
	setNoWrap(boolean)	
HtmlHeader	NORMAL_BODY	
MultiSelect	isLockhart()	
	setLockhart(boolean)	
WizardPanel	setPreviousLabel(String)	setPrevLabel(String)

com.waveset.util.JSSE

Verworfene Methode	Nachfolger
installIfAvailable()	

com.waveset.util.PdfReportRenderer

Verworfene Methode	Nachfolger
render(Element,boolean,String,OutputStream)	render(Element,boolean,String,OutputStream,String, boolean)
render(Element,boolean,String)	render(Element,boolean,String,String,boolean)
render(Report,boolean,String,OutputStream)	render(Report,boolean,String,OutputStream,String, boolean)
render(Report,boolean,String)	render(String,boolean,String,String,boolean)

com.waveset.util.Quota

Verworfene Methode	Nachfolger
getQuota()	

com.waveset.util.ReportRenderer

Verworfene Methode	Nachfolger
renderToPdf(Report,boolean,String,OutputStream)	renderToPdf(Report,boolean,String,OutputStream,String, boolean)
renderToPdf(Report,boolean,String)	renderToPdf(Report,boolean,String,String,boolean)

com.waveset.util.Trace

Verworfene Methode	Nachfolger
data(long,Object,String,byte[])	com.sun.idm.logging.trace.Trace#data(long,String,byte[])
entry(long,Object,String,Object[])	com.sun.idm.logging.trace.Trace#entry(long,String,Object[])
entry(long,Object,String,String)	com.sun.idm.logging.trace.Trace#entry(long,String)
entry(long,Object,String)	com.sun.idm.logging.trace.Trace#entry(long,String)
exception(long,Object,String,t)	com.sun.idm.logging.trace.Trace#throwing(long,String,Throwable) com.sun.idm.logging.trace.Trace#caught(long,String,Throwable)
exit(long,Object,String,boolean)	com.sun.idm.logging.trace.Trace#exit(long,String,boolean)
exit(long,Object,String,int)	com.sun.idm.logging.trace.Trace#exit(long,String,int)
exit(long,Object,String,long)	com.sun.idm.logging.trace.Trace#exit(long,String,long)
exit(long,Object,String,Object)	com.sun.idm.logging.trace.Trace#exit(long,String,Object)
exit(long,Object,String)	com.sun.idm.logging.trace.Trace#exit(long,String)
getTrace()	com.sun.idm.logging.trace.TraceManager#getTrace(String)
getTrace(Class)	com.sun.idm.logging.trace.TraceManager#getTrace(String)
getTrace(String)	com.sun.idm.logging.trace.TraceManager#getTrace(String)
level1(Class,String)	com.sun.idm.logging.trace.Trace#level1(String)
level1(Object,String)	com.sun.idm.logging.trace.Trace#level1(String)
level2(Class,String)	com.sun.idm.logging.trace.Trace#level2(String)
level2(Object,String)	com.sun.idm.logging.trace.Trace#level2(String)
level3(Class,String)	com.sun.idm.logging.trace.Trace#level3(String)
level3(Object,String)	com.sun.idm.logging.trace.Trace#level3(String)
level4(Class,String)	com.sun.idm.logging.trace.Trace#level4(String)
level4(Object,String)	com.sun.idm.logging.trace.Trace#level4(String)
variable(long,Object,String,String,boolean)	com.sun.idm.logging.trace.Trace#variable(long,String,String,boolean)
variable(long,Object,String,String,int)	com.sun.idm.logging.trace.Trace#variable(long,String,String,int)
variable(long,Object,String,String,long)	com.sun.idm.logging.trace.Trace#variable(long,String,String,long)
variable(long,Object,String,String,Object)	com.sun.idm.logging.trace.Trace#variable(long,String,String,Object)
void info(long,Object,String,String)	com.sun.idm.logging.trace.Trace#info(long,String,String)

com.waveset.util.Util

Verworfene Methode	Nachfolger
DATE_FORMAT_CANONICAL	stringToDate(String,String) getCanonicalDate(Date) getCanonicalDate(Date,TimeZone) getCanonicalDate(long)
debug(Object)	
getCanonicalDateFormat()	stringToDate(String,String) getCanonicalDate(Date) getCanonicalDate(Date,TimeZone) getCanonicalDate(long)
getOldCanonicalDateString(Date,boolean)	getCanonicalDateString(Date)
rfc2396URLPieceEncode(String,String)	com.waveset.util.RFC2396URLPieceEncode#encode (String,String)
rfc2396URLPieceEncode(String)	com.waveset.util.RFC2396URLPieceEncode#encode (String)

com.waveset.workflow.WorkflowContext

Verworfene Methode	Nachfolger
VAR_CASE_TERMINATED	com.waveset.object.WFProcess#VAR_CASE_ TERMINATED

Erweiterungen und Korrekturen der Dokumentation

Dieser Abschnitt enthält neue und korrigierte Informationen, die nach der Veröffentlichung der Dokumentation von Identity Manager 7.0 verfügbar wurden. Diese Informationen sind folgendermaßen strukturiert:

Identity Manager Installation

Dieser Abschnitt enthält neue Informationen und Korrekturen an der Dokumentation für *Versionshinweise für Sun Java™ System Identity Manager Installation*.

Neue Funktionen

Zu *Identity Manager Installation* wurden die folgenden neuen Informationen hinzugefügt:

- Da Identity Auditor und Identity Manager SPE in den Identity Manager integriert wurden, sind die Installationsprogramme für diese früheren Module entfernt worden.
- Es wurde ein Kapitel hinzugefügt, das die Installation von Identity Manager auf einem JBoss-Anwendungsserver beschreibt.

Aktualisierungen

Dieser Abschnitt enthält korrigierte Informationen für den Abschnitt *Identity Manager Installation*:

- In Kapitel 1, „Before You Install", muss MySQL 5.0 als unterstütztes Repository aufgeführt werden. Tomcat 5.5 muss als unterstützter Anwendungsserver erscheinen.
- In Kapitel 12, „Uninstalling Applications", muss Schritt 3 des Abschnitts „On UNIX" wie folgt lauten:

  3. Enter the following command:

  ```
  JAVA uninstall_Sun_Java_System_Identity_Manager
  ```

Identity Manager Upgrade

Dieser Abschnitt enthält neue Informationen zu und Korrekturen an der Dokumentation für *Versionshinweise für Sun Java™ System Identity Manager Upgrade*.

Neue Funktionen

Zu *Identity Manager Upgrade* wurden die folgenden neuen Informationen hinzugefügt:

- Anweisungen für die Aufrüstung von Repository-Schemas von Identity Manager 6.0 und 7.0 finden Sie im Abschnitt „Deploying the Upgrade in a Test Environment" von Kapitel 3, "Upgrading Identity Manager in a Test Environment".
- Anweisungen für die Aufrüstung von TaskDefinition-Objekten unter Produktionsbedingungen finden Sie im Abschnitt „Changing TaskDefinition Objects in Production" von Kapitel 4, „Upgrading Identity Manager in a Test Environment".
- Aktualisierte Informationen zu empfohlenen Aufrüstungsmöglichkeiten und Richtlinien in Bezug auf das Ende der Gültigkeitsdauer für den Support von Identity Manager Softwareprodukten finden Sie im Abschnitt „Upgrade Paths and End of Service Life" von Kapitel 1, „Overview of the Upgrade Process".

Identity Manager Administration Guide

Dieser Abschnitt enthält neue Informationen zu und Korrekturen an der Dokumentation für *Versionshinweise für Sun Java™ System Identity Manager Administration*.

Neue Funktionen

Im Zuge der Integration mehrerer Dokumentationen (*Identity Auditor Administration*, *Identity Manager Service Provider Edition Administration Addendum* und *Identity Manager Audit Logging*) in den *Identity Manager Administration* Guide wurden in dieser Ausgabe einige neue Kapitel hinzugefügt.

Im *Identity Manager Administration* Guide erscheinen die folgenden neuen Informationen:

- Kapitel 4, Configuration

  Es wurde ein neuer Abschnitt hinzugefügt, der die neuen Massenressourcen-Aktionen und Richtlinien zu globalen Ressourcen beschreibt.

- Kapitel 5, Administration

  Informationen zum Verstehen und Verwalten von Administrationsrollen und -funktionen wurden vom Kapitel „Configuration" in das Kapitel „Administration" verlegt.

- Kapitel 7, Reporting

  Neue Informationen zur Verwendung von Bedienfeldern zum Gruppieren und Anzeigen grafischer Berichte (vorher im *Identity Manager Service Provider Edition Administration Addendum* enthalten) wurden zu diesem Kapitel hinzugefügt. Weiterhin wurde zu den Berichtstypen der Typ „Auditor Bericht" hinzugefügt.

- Kapitel 11, Identity Auditing

  Dieses neue Kapitel beschreibt die jetzt in Identity Manager enthaltenen Funktionen zur Identitätsüberprüfung. Hier wird erläutert, wie Identitätsüberprüfungen durchgeführt werden, auf Prüfungen zugegriffen werden kann und Benutzerkonformitätsdaten verwaltet werden können.

- Kapitel 12, Audit Logging

  Informationen des Abschnitts „Audit Logging" sind jetzt im *Identity Manager Administration* Guide enthalten. Darüber erscheinen die Tabellen, die unterstützte Datenschemawerte im Überprüfungsprotokoll enthalten, jetzt in Anhang C, „Audit Log Database Schema".

- Kapiel 13, Service Provider Administration

  Dieses neue Kapitel beschreibt, wie die Service Provider-Funktionen Identity Manager konfiguriert und Service Provider-Benutzer (ein neuer Benutzertyp in Identity Manager) verwaltet werden können.

- Anhang D, Active Sync Wizard

  Der Active Sync-Assistent wird ab Version 7.0 nicht mehr unterstützt. Anweisungen zur Verwendung des Active Sync-Assistenten zur Synchronisierungskonfiguration sind jetzt in Anhang D enthalten. Die Synchronisierung wird jetzt gemäß der im Abschnitt „Configuring Synchronization“ von Kapitel 6, „Data Synchronization and Loading“ aufgeführten Synchronisierungsrichtlinien konfiguriert.

Aktualisierungen

In diesem Abschnitt sind Korrekturen an der Dokumentation von *Identity Manager Administration* aufgeführt.

- Identity Manager bietet jetzt mehrere neue Ereignisse, die in Diagrammen oder Tabellen verfolgt und angezeigt werden können:

  - **Provisioner-Ausführungszahl**: Verfolgt, wieviele Provisioner-Vorgänge (nach Vorgangstyp geordnet) aufgetreten sind.
  - **Provisioner-Ausführungsdauer**: Verfolgt die Dauer jedes Provisioner-Vorgangs (nach Vorgangsstyp geordnet).
  - **Anzahl Ressourcenvorgänge**: Verfolgt die Anzahl von Ressourcenvorgängen.
  - **Dauer des Ressourcenvorgangs**: Verfolgt die Dauer von Ressourcenvorgängen.
  - **Workflow-Dauer**: Verfolgt, wie lange die Ausführung eines Workflows dauert.
  - **Workflow-Ausführungsdauer**: Verfolgt, wie oft jeder Workflow ausgeführt wurde.

  Beim Erstellen eines Bedienfelddiagramms können diese Ereignisse aus dem Menü „Ereignisverfolgung“ auf der Seite „Bedienfelddiagramm“ ausgewählt werden:

  a. Wählen Sie in der Administratorbenutzeroberfläche von Identity Manager „Berichte > Bedienfelddiagramme“.

  b. Gehen Sie an das Ende der Bedienfelddiagramme und klicken Sie auf „Neu“, um ein neues Bedienfelddiagramm zu erstellen.

  c. Geben Sie in das Feld „Diagrammname“ einen Namen ein, und wählen Sie dann im Menü „Registry“ die Option „IDM“.

d. Wenn das Menü „Ereignisverfolgung“ angezeigt wird, können Sie aus diesem Menü ein Ereignis auswählen.

Für jedes der verfolgten Ereignisse sind verschiedene Parameter erforderlich. Geben Sie die erforderlichen Parameter ein und klicken Sie dann auf “Speichern”.

e. Starten Sie einige Workflows und überprüfen Sie, ob im Bedienfelddiagramm die entsprechenden Informationen angezeigt werden.

Kapitel 2, Getting Started

Die im Abschnitt zur Benutzeroberfläche von Identity Manager enthaltene Beschreibung zur Option „Anforderungen“ (Requests) muss wie folgt lauten:

> Requests — Submit requests for updates to user account resource assignments and role assignments.

Kapitel 3, User and Account Management

In der Registerkarte „Konten > Konten auflisten“ zur Identitätsüberprüfung stehen jetzt zwei neue Benutzeraktionen zur Verfügung:

- Protokollierte Konformitätsverletzungen anzeigen — Anzeigen von Konformitätsverletzungen, die im Überprüfungsprotokoll des ausgewählten Benutzers erscheinen.

  Sie können eine Zeitdauer oder ein Datum bzw. eine Uhrzeit für die Protokolleinträge eingeben, die angezeigt werden sollen. Sie können auch die Erstellung eines E-Mail-Berichts anfordern. Sie sollten jedoch daran denken, dass in einer solchen E-Mail vertrauliche Informationen (beispielsweise Konto-IDs oder Kontoverlauf) frei zugänglich sein können. Bei Bedarf können Sie die PDF-Standardoptionen für den Bericht überschreiben.

- Konformitätsstatus anzeigen — Anzeigen von Informationen zum aktuellen Status von Konformitätsaktivitäten für einen ausgewählten Benutzer. Diese Aktion meldet das Datum und die Uhrzeit des letzten Überprüfungsrichtlinienabfragen, die zugehörigen Überprüfungsrichtlinie sowie Einzelheiten zu Ausnahmen von den Richtlinien und aufgetretene Richtlinienverletzungen für den betreffenden Benutzer.

Diese Optionen befanden sich ursprünglich im Identity Auditor (Registerkarte Compliance > User).

Kapitel 6, Data Synchronization and Loading

Während des Ladens können jetzt Identity-Attribute angewendet werden.

Dazu müssen Sie zur Liste aktivierter Anwendungen für Identity-Attribute die Optionen „Aus Datei laden“ bzw. „Aus Ressource laden“ hinzufügen.

Wenn sie aktiviert sind, zeigt der Ladevorgang folgende Optionen nicht an:

- Benutzerformular
- Attribute aktualisieren
- Attribute kombinieren

Bei Auswahl der Option „Konten aktualisieren“ werden alle Identity-Attribute vollständig ausgewertet und Konten entsprechend bereitgestellt. Andernfalls werden nur Attribute, die aus der geladenen Datei bzw. Ressource stammen und zum zugehörigen Benutzer gehören, berücksichtigt.

Kapitel 9, Password Sync

JMS Listener-Adapter zur Passwortsynchronisierung werden jetzt in der Metaansicht und nicht mehr mithillfe des ActiveSync-Assistenten konfiguriert.

So konfigurieren Sie einen JMS Listener-Adapter zur Passwortsynchronisierung:

1. Melden Sie sich bei der Identity Manager-Administratorbenutzeroberfläche an.
2. Klicken Sie auf „Metaansicht > Identity-Attribute“.
3. Fügen Sie die folgenden Attribute hinzu:
   - accountID — Wählen Sie zunächst im Feld „Attributname“ dieses Attribut und dann aus der JMS-Ressource das Attribut „IDMAccountid“ aus.
   - Passwort — Wählen Sie zunächst im Feld „Attributname“ dieses Attribut und dann aus der JMS-Ressource das Attribut „Passwort“ aus.
4. Stellen Sie die gewünschten Attributeigenschaften ein. Weitere Informationen zum Einstellen von Attributeigenschaften finden Sie im Abschnitt “Adding and Editing Identity Attributes” in Kapitel 3 des *Identity Manager Administration* Guide.
5. Geben Sie gewünschte Ziele an. Sie können beispielsweise LDAP-Ziele hinzufügen oder die Bedingungen für Zielattribute anpassen.
6. Klicken Sie auf OK, um zur Seite „Identity-Attribute“ zurückzukehren.
7. Wählen Sie im Bereich „Aktivierte Anwendungen“ die Anwendung „Active Sync“ aus.
8. Klicken Sie auf „Speichern“.
9. Folgen Sie den Anweisungen im Abschnitt “Configuring Synchronization” für Active Sync-Adapters in Kapitel 6 in *Identity Manager Administration*, um Synchronisierungen für JMS Listener-Adapter zu konfigurieren.

Kapitel 11, Identity Auditing

- Im Abschnitt „Attestation Security“, Kapitel „Identity Auditing“, fehlt der folgende Hinweis:

  Note: If security on Attestations is set to organization controlled, then the Auditor Attestor capability is also required to modify another user's attestations.

- Der im Abschnitt “Adjust Escalation Timeouts” aufgeführte Standardwert für den Parameter „Eskalationszeitüberschreitung“ muss richtig 7 Tage lauten.

Identity Manager Resources Reference

Dieser Abschnitt enthält neue Informationen zu und Korrekturen an der Dokumentation für *Versionshinweise für Sun Java™ System Identity Manager Resources Reference*.

Neue Funktionen

Zu *Identity Manager Resources Reference* wurden die folgenden neuen Informationen hinzugefügt:

- BridgeStream SmartRoles-Adapter
- Skript- JDBC-Adapter
- Realm-Unterstützung in Sun Java System Access Manager

Aktualisierungen

In der Tabelle „Provisioning Notes“ für den Shell-Skript-Adapter muss erwähnt werden, dass Konten aktiviert und deaktiviert werden können.

Identity Manager Technical Deployment Overview

Dieser Abschnitt enthält neue Informationen zu und Korrekturen an der Dokumentation für *Versionshinweise für Sun Java™ System Identity Manager Technical Deployment Overview*.

Neue Funktionen

Zu *Identity Manager Technical Deployment Overview* wurden die folgenden neuen Informationen hinzugefügt:

- eine Erläuterung zur Behandlung mehrerer Konten für einen einzelnen Identity Manager-Benutzer auf einer Ressource (Anhang C, „Assigning Multiple Accounts per User to a Resource“)
- Aktualisierungen zu den Prozessen zur privaten Benennung von Softwareschnittstellen (Kapitel 5., Private Labelling of Identity Manager)
- eine Erläuterung zum Erstellen eines Links auf die Anmeldeseite in jeder verfügbaren Sprache (Anhang B, „Enabling Internationalization“)

Aktualisierungen

In diesem Abschnitt sind Korrekturen zu *Identity Manager Technical Deployment Overview* aufgeführt.

- Mit CSS können Sie die Spaltenbreiten der Benutzerliste und der Ressourcenlistentabellen auf einen festen Pixelwert oder einen Prozentsatz einstellen. Fügen Sie dazu zur Datei `customStyle.css` die folgenden (standardmäßig auskommentierten) Stilklassen hinzu. Sie können dann deren Werte je nach den Benutzeranforderungen entsprechend ändern.

```
th#UserListTreeContent_Col0 {
            width: 1px;
}

th#UserListTreeContent_Col1 {
            width: 1px;
}

th#UserListTreeContent_Col2 {
            width: 50%;
}

th#UserListTreeContent_Col3 {
            width: 50%;
}

th#ResourceListTreeContent_Col0 {
            width: 1px;
}

th#ResourceListTreeContent_Col1 {
            width: 1px;
}

th#ResourceListTreeContent_Col2 {
            width: 33%;
}

th#ResourceListTreeContent_Col3 {
            width: 33%;
}

th#ResourceListTreeContent_Col4 {
            width: 33%;
}
```

Sie können darüber hinaus Tabellenspaltenbreiten durch Klicken und Ziehen der Begrenzung der entsprechenden Spaltenüberschrift ändern. Wenn Sie die Maus auf die rechte Begrenzung einer Spaltenüberschrift setzen, wird der Cursor als horizontaler Größenänderungspfeil angezeigt. Die Spaltenbreite kann durch Klicken mit der linken Maustaste und Ziehen des Mauszeigers geändert werden. Bei Freigabe der Maustaste ist die Breitenänderung beendet.

- Das Objekt „System Configuration" enthält jetzt das Attribut `security.delegation.historyLength`, das die Anzahl der vorher protokollierten Delegierungen enthält.
- Im Bedienfelddiagramm „Zugriffsprüfungen" und in „Bericht über Zugriffsprüfungsdetails" werden Instanzen von Prüfungen angezeigt, die in der Überprüfungsprotokollierung aufgezeichnet wurden. Ohne eine entsprechende Datenbankpflege werden die Überprüfungsprotokolle niemals geleert, und die Prüfungsliste wird immer länger. Identity Manager bietet die Möglichkeit, die angezeigten Prüfungen auf ein gewisses Alter zu begrenzen. Wenn Sie diese Zeitbegrenzung ändern möchten, müssen Sie die Datei `compliance/dashboard.jsp` (für das Bedienfelddiagramm) bzw. `sample/auditortasks.xml` (für den Bericht über Zugriffsprüfungsdetails) entsprechend anpassen. Standardmäßig werden nur Prüfungen angezeigt, die nicht älter als 2 Jahre sind.

  Zum Einschränken der Anzahl der im Bedienfelddiagramm „Zugriffsprüfungen" angezeigten Prüfungen müssen Sie die Datei `compliance/dashboard.jsp` wie folgt ändern:

  a. Öffnen Sie die Datei `compliance/dashboard.jsp` in der Identity Manager IDE oder in einem Editor Ihrer Wahl:

  b. Ändern Sie die Zeile `form.setOption(„maxAge", „2y");` in `form.setOption(„maxAge", „6M");` wenn nur Prüfungen angezeigt werden sollen, die nicht älter als 6 Monate sind. Folgende Bezeichner existieren:

    - m - Minute
    - h - Stunde
    - d - Tage
    - w - Woche
    - M - Monat
    - y - Jahr

  Wenn alle in den Überprüfungsprotokollen enthaltenen Prüfungen angezeigt werden sollen, müssen Sie diese Zeile auskommentieren.

So begrenzen Sie die Anzahl der im Bericht über Zugriffsprüfungsdetails angezeigten Prüfungen:

a. Öffnen Sie die Datei sample/auditortasks.xml in der IDE oder in einem Editor Ihrer Wahl:

b. Ändern Sie die Zeile

```
<s>maxAge</s>
  <s>2y</s>
```

in

```
<s>maxAge</s>
  <s>6M</s>
```

wenn nur Prüfungen angezeigt werden sollen, die nicht älter als 6 Monate sind. Für diese Datei gelten die gleichen, oben aufgeführten Bezeichner.

Jede regelmäßige Zugriffsprüfung enthält eine Reihe von UserEntitlement-Einträgen, die bei der Ausführung der Prüfung erstellt wurden. Diese mit der Zeit immer zahlreicher werdenden Einträge bieten wertvolle IVerlaufsinformationen zu Konten. Zur Einsparung von Datenbankspeicherplatz sollten einige Einträge jedoch gelöscht werden. Einträge können mit **Serveraufgaben > Aufgabe ausführen > Zugriffsprüfung löschen** gelöscht werden. Durch das Löschen von Zugriffsprüfungen werden neue Überprüfungsprotokolleinträge hinzugefügt, die angeben, dass Zugriffsprüfungen gelöscht wurden, und es werden alle zu diesen Zugriffsprüfungen gehörenden UserEntitlement-Einträge entfernt. Das spart Datenbankspeicherplatz.

- Im Abschnitt “ Changing Background Image on the Login Page” (Kapitel 5) muss die dritte Codezeile wie folgt lauten:

```
url(../images/other/login-backimage2.jpg)
```

- Code-Beispiel 5-5 enthält Informationen, die eigentlich in Code-Beispiel 5-4 gehören. Code-Beispiel 5.4 muss wie folgt lauten:

CODE-BEISPIEL 5.4 Anpassen von Navigationsregisterkarten

```
/* LEVEL 1 TABS */
.TabLvl1Div {
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
    background-color:#333366;
    padding:6px 10px 0px;
}
a.TabLvl1Lnk:link, a.TabLvl1Lnk:visited  {
    display:block;
    padding:4px 10px 3px;
```

CODE-BEISPIEL 5.4 Anpassen von Navigationsregisterkarten *(Fortsetzung)*

```
    font: bold 0.95em sans-serif;
    color:#FFF;
    text-decoration:none;
    text-align:center;
}
table.TabLvl1Tbl td {
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left top;
    background-color:#666699;
    border:solid 1px #aba1b5;
}
table.TabLvl1Tbl td.TabLvl1TblSelTd {
    background-color:#9999CC;
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
    border-bottom:none;
}

/* LEVEL 2 TABS */
.TabLvl2Div {
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left bottom;
    background-color:#9999CC;
    padding:6px 0px 0px 10px
}
a.TabLvl2Lnk:link, a.TabLvl2Lnk:visited{
    display:block;
    padding:3px 6px 2px;
    font: 0.8em sans-serif;
    color:#333;
    text-decoration:none;
    text-align:center;
}
table.TabLvl2Tbl div.TabLvl2SelTxt {
    display:block;
    padding:3px 6px 2px;
    font: 0.8em sans-serif;
    color:#333;
    font-weight:normal;
    text-align:center;
}
table.TabLvl2Tbl td {
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
    background-position:left top;
    background-color:#CCCCFF;
    border:solid 1px #aba1b5;
}
table.TabLvl2Tbl td.TabLvl2TblSelTd {
    border-bottom:none;
    background-image:url(../images/other/dot.gif);
    background-repeat:repeat-x;
```

CODE-BEISPIEL 5.4 Anpassen von Navigationsregisterkarten *(Fortsetzung)*

```
    background-position:left bottom;
    background-color:#FFF;
    border-left:solid 1px #aba1b5;
    border-right:solid 1px #aba1b5;
    border-top:solid 1px #aba1b5;
```

Code-Beispiel 5.5 muss wie folgt lauten:

CODE-BEISPIEL 5.5 Ändern von Registerkartenfeldern

```
table.Tab2TblNew td
{background-image:url(../images/other/dot.gif);background-repeat:repeat-x;background-positi
on:left top;background-color:#CCCCFF;border:solid 1px #8f989f}
table.Tab2TblNew td.Tab2TblSelTd
{border-bottom:none;background-image:url(../images/other/dot.gif);background-repeat:repeat-
x;background-position:left bottom;background-color:#FFF;border-left:solid 1px
#8f989f;border-right:solid 1px #8f989f;border-top:solid 1px #8f989f}
```

Identity Manager Workflows, Forms, and Views

Dieser Abschnitt enthält neue Informationen zu und Korrekturen an der Dokumentation für *Versionshinweise für Sun Java™ System Identity Manager Workflows, Forms, and Views*.

Neue Funktionen

Zu *Identity Manager Workflows, Forms, and Views* wurden die folgenden neuen Informationen hinzugefügt:

- eine Erläuterung der FormUtil-Methode `getSubordinates` (Kapitel 4, „FormUtil Methods“).
- eine bessere Erläuterung der XPRESS-Funktion `<set>` und zugehöriger Funktionen (Kapitel 6, „XPRESS Language“).
- eine Erläuterung der HTML-Anzeigekomponente `inlineAlert` (Kapitel 8, „HTML Display Components“).
- eine Erläuterung, wie die automatische Verknüpfung vorhandener Konten deaktiviert werden kann (Kapitel 3, „Identity Manager Forms“).

Aktualisierungen

In diesem Abschnitt sind Korrekturen an der Dokumentation von *Identity Manager Workflows, Forms, and Views* aufgeführt.

- Das Überprüfen von Richtlinien in Benutzerformularen kann durch Hinzufügen der folgenden Zeile zum Formular deaktiviert werden:

```
<Field name='viewOptions.CallViewValidators'>
  <Display class='Hidden'/>
    <Expansion>
        <s>false</s>
    </Expansion>
</Field>
```

Dieses Feld hat Vorrang vor dem Wert des Feldes OP_CALL_VIEW_VALIDATORS in der Datei `modify.jsp`.

- Die Seiten der Benutzeroberfläche von Identity Manager enthalten ein zweites XPRESS-Formular, das eine Navigationsleiste implementiert. Deswegen enthält die ausgegebene Seite zwei `<FORM>`-Tags mit verschiedenen Name-Attributen:

  `<form name="endUserNavigation">` und `<form name="mainform">`

  Zum Vermeiden von Verwechslungen zwischen diesen beiden `<FORM>`-Tags müssen Sie sicherstellen, dass das Attribut `name` wie folgt verwendet wird, damit eindeutig wird, welches `<FORM>`-Tag gemeint ist: `document.mainform` oder `document.endUserNavigation`.

- Die Erläuterung des Elements `Field` in Kapitel 3, „Identity Manager Forms", muss die folgende Beschreibung des Attributs `confirm` enthalten.

  `confirm` - Use to ensure that the values of two fields match when the form is submitted. The value of this attribute should be the name of another field defined in the form whose value this field is expected to match.

Identity Manager Deployment Tools

Dieser Abschnitt enthält neue Informationen zu und Korrekturen an der Dokumentation für *Versionshinweise für Sun Java™ System Identity Manager Deployment Tools*.

Neue Funktionen

Zu *Identity Manager Deployment Tools* wurden die folgenden neuen Informationen hinzugefügt:

- Zum Kapitel „Working with Rules" wurden einige neue Regeln für regelmäßige Zugriffsprüfungen hinzugefügt.
- Anweisungen zum Erstellen und Bearbeiten von Regeln mithilfe von BPE wurden von Kapitel 2, „Working with Rules" in den neuen Abschnitt „Creating and Editing Rules" in Anhang A, „Using the Identity Manager BPE" verlegt.
- Im neuen Kapitel 1, „Using the Identity Manager IDE" wird die Installation und Verwendung der neuen Identity Manager Integrated Development Environment (Identity Manager IDE) beschrieben.

  Bei dieser Java-Anwendung handelt es sich um ein vollständig integriertes NetBeans-Plugin, mit dem Sie Identity Manager-Objekte in Ihrem Deployment anzeigen und anpassen sowie darin Fehler suchen können. Die Identity Manager IDE löst den Business Process Editor (BPE) von Identity Manager ab.

- Das vorhandene Kapitel „Using the Identity Manager BPE“ wurde in einen Anhang umgewandelt.
- Das neue Kapitel 8, „Using SPML 2.0 with Identity Manager Web Services“ beschreibt die neue Unterstützung für SPML 2.0 in Identity Manager; u.a., welche Funktionen warum unterstützt werden. Darüber hinaus finden Sie hier Anweisungen zur Konfiguration der SPML 2.0-Unterstützung, und wie diese Unterstützung in der Praxis ausgebaut werden kann.

Identity Manager Tuning, Troubleshooting, and Error Messages

Dieser Abschnitt enthält neue Informationen zu und Korrekturen an der Dokumentation für *Versionshinweise für Sun Java™ System Identity Manager Tuning, Troubleshooting, and Error Messages*.

Neue Funktionen

Zu *Identity Manager Tuning, Troubleshooting, and Error Messages* wurden die folgenden neuen Informationen hinzugefügt:

- Informationen zum Verfolgen von Autorisierungsflüssen beim Anzeigen bzw. Zugreifen auf Service Provider-Benutzer sowie beim Zuweisen von Admin-Rollen bei der Anmeldung als Service Provider-Benutzer (siehe neuer Abschnitt „SPE Delegated Administration Tracing“ in Kapitel 2, „Troubleshooting and Tracing“).
- Anweisungen zum Anzeigen von SystemLog-Berichten finden Sie im Abschnitt „Viewing SystemLog Reports“ von Kapitel 3, „Errors and Exceptions“.
- Informationen zum neuen Format und der neuen Darstellung von Fehlermeldungen finden Sie im Abschnitt „Overview“ von Kapitel 3, „Errors and Exceptions“.

Aktualisierungen

Einige Aufgaben wurden vom Adapter- in das Aufgaben-Package verlegt. Wenn Sie für die folgenden Aufgaben Verfolgungen aktiviert oder Aufgaben definiert haben, die auf diese Packages verweisen, müssen Sie Pfade entsprechend aktualisieren.

Alte Package-Bezeichnung	Neue Package-Bezeichnung
com.waveset.adapter.ADSyncFailoverTask	com.waveset.task.ADSyncFailoverTask
com.waveset.adapter.ADSyncRecoveryCollectorTask	com.waveset.task.ADSyncRecoveryCollectorTask
com.waveset.adapter.SARunner	com.waveset.task.SARunner
com.waveset.adapter.SourceAdapterTask	com.waveset.task.SourceAdapterTask

Identity Manager Service Provider Edition Deployment

Dieser Abschnitt enthält neue Informationen zu und Korrekturen an der Dokumentation für *Versionshinweise für Sun Java™ System Identity Manager SPE Deployment*.

Neue Funktionen

- Identity Manager and Identity Manager SPE nutzen jetzt das gleiche Überprüfungssystem. Deswegen sind Erläuterungen zu Überprüfungen jetzt in *Identity Manager Deployment Tools* enthalten.
- Identity Manager SPE nutzt jetzt anstatt des IDMXContext den LighthouseContext. Deswegen wurde das Kapitel zu IDMXContext entfernt.

Arbeiten mit helpTool

Identity Manager 6.0 enthält eine neue Funktion zum Durchsuchen der Onlinehilfe und der Dokumentation im HTML-Format. Das Suchmodul basiert auf der Nova-Suchmaschinentechnologie von SunLabs.

Die Verwendung des Nova-Suchmoduls verläuft in zwei Phasen: *Indizierung* und *Abruf*. Während der Indizierung werden die Eingabedokumente analysiert und es wird ein Index für die Abrufphase erstellt. Während des Abrufs können „Passagen" abgerufen werden, die aus dem Kontext bestehen, in dem die Abfragebegriffe gefunden wurden. Der Abrufprozess für die Passagen benötigt die ursprünglichen HTML-Dateien. Diese Dateien müssen sich deshalb in einem Verzeichnis des Dateisystems befinden, auf das das Suchmodul Zugriff hat.

helpTool ist ein Java-Programm, das zwei grundlegende Funktionen ausführt:

- Kopieren der HTML-Quelldateien in einen Speicherort, auf das das Suchmodul Zugriff hat
- Erstellen des Index für die Abrufphase

helpTool wird folgendermaßen über die Befehlszeile ausgeführt:

```
$ java -jar helpTool.jar
usage: HelpTool
 -d    Destination directory
 -h    This help information
 -i    Directory or JAR containing input files, no wildcards
 -n    Directory for Nova index
 -o    Output file name
 -p    Indexing properties file
```

Neuerstellung des Onlinehilfe-Index

Die HTML-Dateien für die Onlinehilfe sind in einer JAR-Datei als Paket enthalten. Sie müssen diese Dateien in ein Verzeichnis für das Suchmodul extrahieren. Gehen Sie folgendermaßen vor:

1. Entpacken Sie das helpTool-Paket in ein temporäres Verzeichnis. (Details werden später angegeben).

   In diesem Beispiel werden die Dateien in das Verzeichnis `/tmp/helpTool` extrahiert.

2. Geben Sie in einer UNIX-Shell oder in einem Windows-Befehlsfenster das Verzeichnis an, in dem die Identity Manager-Anwendung Ihrem Webcontainer bereitgestellt wurde.

   Es kann beispielsweise folgendes Verzeichnis für Sun Java System Application Server verwendet werden:

   ```
   /opt/SUNWappserver/domains/domain1/applications/j2ee-modules/idm
   ```

3. Verwenden Sie `help/` als aktuelles Arbeitsverzeichnis.

   HINWEIS Sie müssen helpTool unbedingt von diesem Verzeichnis ausführen, da andernfalls der Index nicht korrekt erstellt wird. Entfernen Sie außerdem durch Löschen des Inhalts des Verzeichnisses `index/help/` die alten Indexdateien.

4. Erfassen Sie folgende Informationen für Ihre Befehlszeilenargumente:

   - **Zielverzeichnis —** `html/help/en_US`

     HINWEIS Verwenden Sie die für Ihre Installation geeignete Gebietsschemazeichenfolge.

   - **Eingabedatei —** `../WEB-INF/lib/idm.jar`
   - **Nova-Indexverzeichnis —** `index/help`
   - **Name der Ausgabedatei —** `index_files_help.txt`

     HINWEIS Dieser Dateiname ist nicht wichtig, das Tool wird jedoch beendet, falls diese Datei bereits vorhanden ist.

   - **Eigenschaftendatei für die Indizierung —** `index/index.properties`

5. Führen Sie folgenden Befehl aus:

```
$ java -jar /tmp/helpTool/helpTool.jar -d html/help/en_US -i ../
WEB-INF/lib/idm.jar -n index/help -o help_files_help.txt -p index/index.properties

Extracted 475 files.

[15/Dec/2005:13:11:38] PM Init index/help AWord 1085803878

[15/Dec/2005:13:11:38] PM Making meta file: index/help/MF: 0

[15/Dec/2005:13:11:38] PM Created active file: index/help/AL

[15/Dec/2005:13:11:40] MP Partition: 1, 475 documents, 5496 terms.

[15/Dec/2005:13:11:40] MP Finished dumping: 1 index/help 0.266

[15/Dec/2005:13:11:40] IS 475 documents, 6,56 MB, 2,11 s, 11166,66 MB/h

[15/Dec/2005:13:11:40] PM Waiting for housekeeper to finish

[15/Dec/2005:13:11:41] PM Shutdown index/help AWord 1085803878
```

Neuerstellung des Dokumentationsindex

Gehen Sie folgendermaßen vor, um den Dokumentationsindex neu zu erstellen:

1. Entpacken Sie das helpTool-Paket in ein temporäres Verzeichnis. (Details werden später angegeben)

   In diesem Beispiel werden die Dateien in das Verzeichnis `/tmp/helpTool` extrahiert.

2. Geben Sie in einer UNIX-Shell oder in einem Windows-Befehlsfenster das Verzeichnis an, in dem die Identity Manager-Anwendung Ihrem Webcontainer bereitgestellt wurde.

   Es kann beispielsweise folgendes Verzeichnis für Sun Java System Application Server verwendet werden:

   ```
   /opt/SUNWappserver/domains/domain1/applications/j2ee-modules/idm
   ```

3. Verwenden Sie `help/` als aktuelles Arbeitsverzeichnis.

   HINWEIS Sie müssen helpTool unbedingt von diesem Verzeichnis ausführen, da andernfalls der Index nicht korrekt erstellt wird. Entfernen Sie außerdem die alten Indexdateien, indem Sie den Inhalt des Verzeichnisses `index/docs/` löschen.

4. Erfassen Sie folgende Informationen für Ihre Befehlszeilenargumente:

   - **Zielverzeichnis —** `html/docs`
   - **Eingabedateien —** `../doc/HTML/en_US`

     HINWEIS Das Tool kopiert das Verzeichnis `en_US/` und dessen Unterverzeichnisse in dieses Ziel.

   - **Nova-Indexverzeichnis —** `index/docs`
   - **Name der Ausgabedatei —** `index_files_docs.txt`

     HINWEIS Dieser Dateiname ist nicht wichtig, das Tool wird jedoch beendet, falls diese Datei bereits vorhanden ist.

   - **Eigenschaftendatei für die Indizierung —** `index/index.properties`

5. Führen Sie folgenden Befehl aus:

```
$ java -jar /tmp/helpTool/helpTool.jar -d html/docs -i ../doc/HTML/en_US -n index/docs
-o help_files_docs.txt -p index/index.properties
Copied 84 files.
Copied 105 files.
Copied 1 files.
Copied 15 files.
Copied 1 files.
Copied 58 files.
Copied 134 files.
Copied 156 files.
Copied 116 files.
Copied 136 files.
Copied 21 files.
Copied 37 files.
Copied 1 files.
Copied 13 files.
Copied 2 files.
Copied 19 files.
Copied 20 files.
Copied 52 files.
Copied 3 files.
Copied 14 files.
Copied 3 files.
Copied 3 files.
Copied 608 files.
[15/Dec/2005:13:24:25] PM Init index/docs AWord 1252155067
[15/Dec/2005:13:24:25] PM Making meta file: index/docs/MF: 0
[15/Dec/2005:13:24:25] PM Created active file: index/docs/AL
[15/Dec/2005:13:24:28] MP Partition: 1, 192 documents, 38488 terms.
[15/Dec/2005:13:24:29] MP Finished dumping: 1 index/docs 0.617
[15/Dec/2005:13:24:29] IS 192 documents, 14.70 MB, 3.81 s, 13900.78 MB/h
[15/Dec/2005:13:24:29] PM Waiting for housekeeper to finish
[15/Dec/2005:13:24:30] PM Shutdown index/docs AWord 1252155067
```